Security & Compliance

Adaface

Web version of our whitepaper:

Trust Guide

Privacy

Privacy Policy

Security

Control Visibility

Information Security

Architecture

Compliance

Cookie Policy

GDPR Commitment

GDPR FAQs

Security Practices

Data Management

Data Residency

Data requests

We are committed to the security and privacy of your data

Trust is the foundation of our relationship with millions of candidates and businesses around the world. We value the confidence you've put in us and take the responsibility of protecting your information seriously. To be worthy of your trust, we built and will continue to grow Adaface with an emphasis on security, compliance, and privacy.

Our Trust Guide connects you to our privacy, security and compliance programmes, so you have all of the information that you need to manage your data.

Privacy

You own your data, and whether it's your personal or work information, we're committed to keeping it private. Our policies, tools and procedures are built to protect your data and help you to meet your privacy obligations.

Security

Adaface is designed with a secure, distributed infrastructure with multiple layers of protection. We work behind the scenes to imbibe enterprise-grade security into every aspect of how recruiters collaborate for screening.

Compliance

Our robust programme complies with regulations like GDPR and CCPA and can help you navigate your compliance. Our internal auditors test our controls to ensure all compliance layers are secure and consistent with our policies.

Data Management

Our data management infrastructure is designed with operational, technical, and procedural security controls. We are committed to providing transparency into the policies and tools that affect how you manage your data.

Data Requests

We're committed to being as transparent as possible about how we manage your information, while making sure we keep it secure and private. Our data request policy provides insight into third-party/ law enforcement requests for data.

Privacy at Adaface

It’s our responsibility to protect your recruiting data and keep it private. Our commitment to your privacy is at the heart of every decision we make. We protect your data and give you the information and tools that you need to meet your privacy obligations.

Own and control the data within your Adaface account

We work hard to protect your information and your candidate's information from unauthorized access and have design policies and controls to safeguard the collection, use and disclosure of your information.

Ownership and retention that work for you and your team

We provide enterprises with tools that can help keep their data private, so we can work together to protect your hiring data. Enterprise recruiters can export, edit and delete their data. They can set retention policies that work for you. For enterprise accounts, we provide control over location of data storage (at an additional cost). You can discuss with your Adaface account manager for more information.

We’re transparent, so that you can have peace of mind

We’re committed to being as transparent as possible about government requests. To this end, have confidence in how Adaface uses personal information, as well as when and how we contact customers.

Compliance with global privacy laws and regulations

We support our customers’ needs through our tooling and contractual commitments. Data privacy features and technologies for enhancing data privacy are embedded directly into the design of our projects and services.

View our privacy policy

Enterprise-grade security

Adaface provides the control and visibility features that recruitment admins need. Behind the scenes is a secure, sophisticated infrastructure built to protect your data while being transferred, stored, and processed. Our information security management framework is designed to assess risks and build a culture of security at Adaface.

Control and visibility

We've developed tools that empower recruiters to customize Adaface to their organization's particular needs. Adaface dashboard provides control and visibility features, and provides tools to protect their accounts across various user interfaces. The Adaface Integration API also allows for partner product integrations with core IT processes. We help you ensure that only the right people can access your company's information in Adaface.

Information security

By default, Adaface encrypts data for all of our customers. We further protect your data with tools such as audit logs, data backups and recovery. We're always assessing risks and improving the security, confidentiality, integrity, and availability of our systems. We regularly review and update security policies, provide our employees with security training, perform application and network security testing (including penetration testing).

Architecture overview

Adaface is designed with multiple layers of protection, including secure data transfer, encryption, network configuration, and application-level controls distributed across a scalable, secure infrastructure. Adaface offers governance and risk-management capabilities flexible enough to meet your organisation's needs, no matter what they are. This includes global retention policies and custom terms of service.

Security control and visibility

We've developed a number of tools that empower enterprise recruiters and IT teams to customize Adaface to their organization's particular security control needs. A toolbox of control and visibility features is available via the Adaface dashboard for super admins. We've also extended the platform to help businesses integrate Adaface seamlessly into their core IT processes with our ATS integrations and Integration API.

Identity and access management

- Directory services integration & Single sign-on (SSO): Enterprises can simplify provisioning and de-provisioning by automatically adding and removing users from existing internal directories. Your Adaface account manager can help you pick the right plans that give you access to our identity management providers and SSO (Single sign-on) capabilities.
- Advanced fraud protection: Super admins can request advanced login protection: This feature ensures users can log in only from one device at a time and identify fraudulent access to your Adaface accounts.

Sharing controls

Super admins of Adaface have comprehensive control of their team's abilities in the Adaface dashboard. This includes whether members can invite other members and give controlled access to different portions of the Adaface dashboard. Super admins can restrict only a set of recruiters to have the capabilities to edit test settings, create new tests and new public links to tests. Users with view-only access to tests can only administer the test to candidates but would not be able to change the proctoring capabilities of a test.

Administrative actions and visibility

Adaface provides an extensive toolbox for super admins to manage your Adaface account and adhere to your organization's internal security policies. Some restricted features of Adaface are only visible to super admins. These include:

- Tracking account usage
- Permanently deleting and anonymizing candidates data
- Deleting, deactivating, and activating other recruiter logins
- Access to hiring insights and usage reports
- Access to complete audit logs
- Access to billing information including downloadable invoices

Additionally, super admins can work with Adaface account managers for any data requests such as account transfer, remote wipe. Note that some of these features are available to only enterprise customers and depend on the plan you subscribe to.

Learn more about user roles and permissions

Automation, Integrations & API

We extended the power of the Adaface Platform through automation and integrations to help businesses integrate Adaface into their core IT processes and support custom workflows. The automation helps recruiters communicate with candidates without the overhead of tracking candidate activity. This includes automated invite, reminder, shortlist and rejection emails. Only a handful of these features are enabled by default. Your account manager works with you to customize our automated features to best fit your recruiting processes. Our ATS (application tracking system) integrations help you administer Adaface assessments without leaving your hiring systems. You can invite a candidate to an assessment, track their assessment progress, view the candidate score and scorecard right within your ATS. To further customize your workflow, we provide an Integration API that gives you access to Adaface features. To know more about pricing and details of our integration API, speak with your Adaface account manager.

Information Security

Learn how Adaface's advanced IT security management helps protect your sensitive information from unauthorized access, phishing, data breaches, and new threats.

Adaface policies safeguard your information

Adaface has strict risk management policies regarding user information assurance. We are committed to ongoing risk assessment and continually improving the security testing, confidentiality, and data integrity of Adaface systems. Key areas include:

- Access and Authentication Requirements
- Content Policies
- Retention and deletion
- Discovery and Classification
- Data Loss Prevention

How Adaface protects your information

Team access controls: Employee access to data is granted based on role based access control and all access requires layers of authentication.

Change management: The Adaface Engineering team’s Formal Change Management Policy ensures that changes have been authorized prior to implementation into production environments.

Infrastructure security: Our underlying infrastructure is designed with modern security concepts like defense in depth and based on a zero trust model. Our security controls are tested extensively by our own security team.

Content and data controls: Adaface safeguards your recruiting data with granular permissions and policies and legal holds.

Information security requires transparency

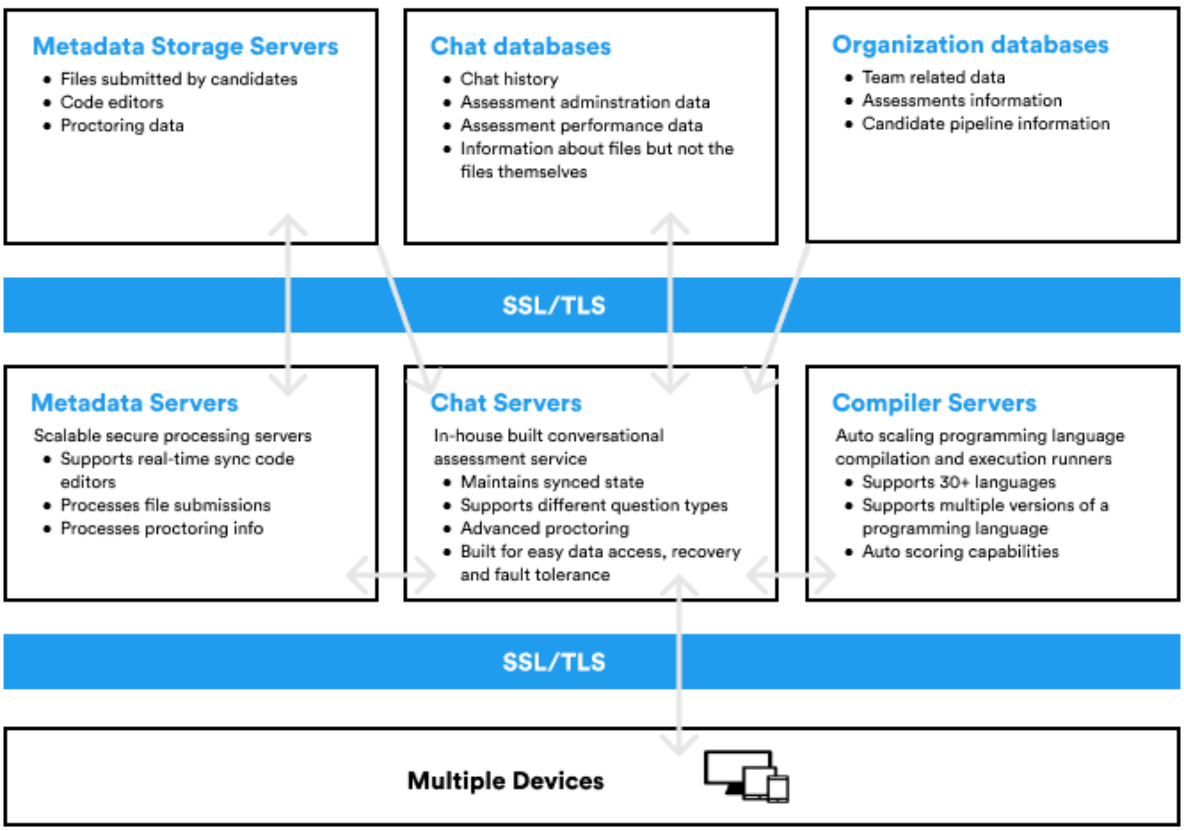
Transparency is everything when it comes to building trust and protecting the rights of our users. To that end, Adaface account managers work with enterprise recruiters to communicate about how we handle government requests for user data.

Architecture Overview

Learn how Adaface's advanced IT security management helps protect your sensitive information from unauthorized access, phishing, data breaches, and new threats.

Chat infrastructure

Candidates can access the conversational assessments they are invited to from any modern browser. Each conversational assessment session has security settings and features that process and protect candidate's data while ensuring ease of access. All of these clients connect to secure servers to provide access to file sharing, code writing, compiling, and engaging with Adaface chatbot, Ada. Our chat infrastructure is comprised of the following components:



Metadata storage servers

Certain information about the conversation with the bot that is useful for creating a good user experience or considered as secondary elements in the overall conversation is called metadata. This metadata includes any files submitted by the user and proctoring information collected by our bot during the assessment. Dedicated storage services are deployed for different types of

secondary data based on function and format. Storage servers with sync support and version history are deployed for relevant data like coding editors used during the chat.

Chat databases

Primary information about the chat is stored in a MySQL-backed database service and is sharded and replicated as needed to meet performance and high availability requirements. Primary conversation data acts as a single source of truth for every conversation with the bot and stores important assessment information helpful in administering the assessment and scoring the candidates' performance.

Organization databases

Organization information critical to conducting a chat - assessment data, customizations, settings, and information required for secure candidate authentication is stored in a MySQL-backed database service and is sharded and replicated as needed to meet performance and high availability requirements.

Metadata servers

The Metadata servers are responsible for cleaning, processing, and serving secondary data collected during the assessment.

Chat servers

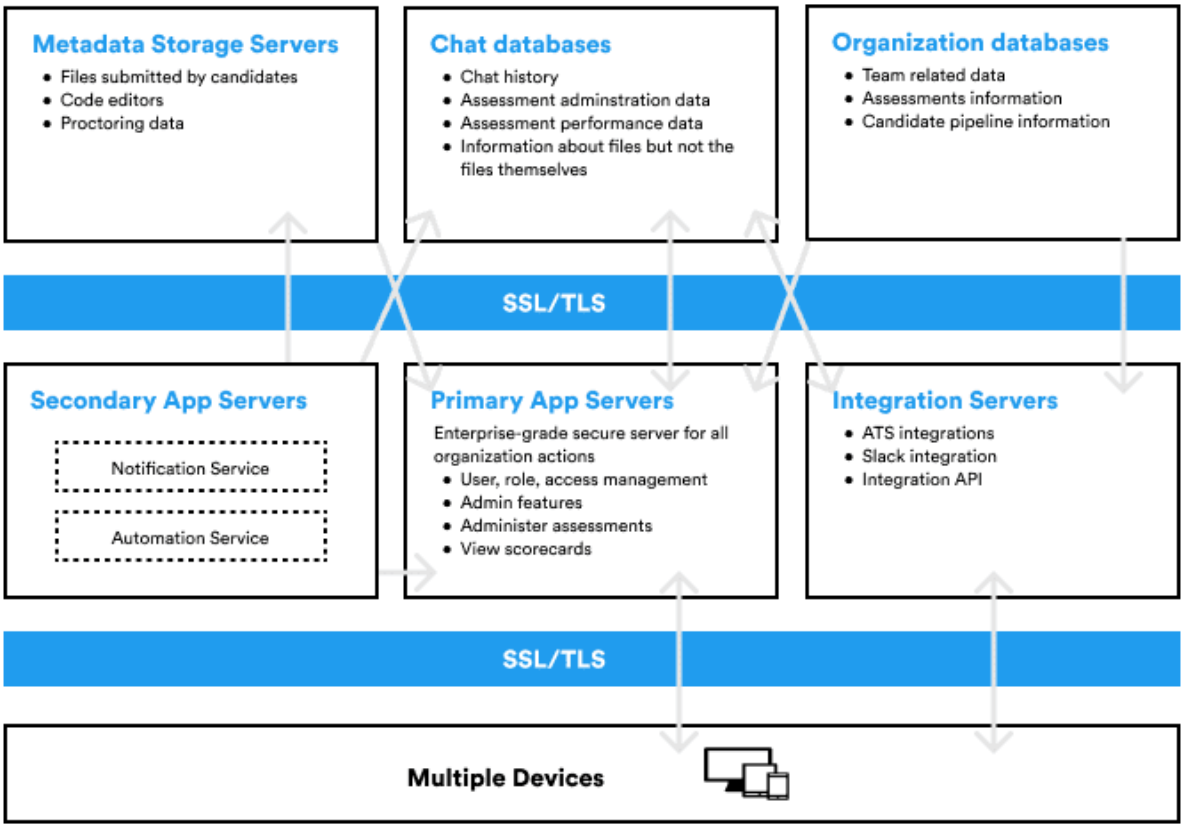
Our chat servers are built to automatically scale based on a surge of concurrent conversational assessments. They handle the logic, data processing, and data synchronization of all primary data collected during the assessment.

Compiler servers

This is a separate service dedicated to supporting code compilers. Adaface conversational assessments support 30+ programming languages. To enable concurrent code execution and compilation functionality for candidates, our compiler services are kept on auto-scale infrastructure.

Dashboard/ App Infrastructure

Adaface recruiters can access their Adaface dashboard/ account at any time from the web and mobile clients, or through third-party applications connected to the Adaface application via our integration APIs. All of these clients connect to secure servers to provide access to the Adaface dashboard, access/ create/ edit Adaface test library, access/ create/ delete candidate invites, view candidate scorecards, and manage the candidate pipeline. Our dashboard infrastructure comprises of following components:



Metadata storage servers

Metadata/Secondary data collected from candidates during the conversational assessment is used by the Adaface application to generate scorecards. This metadata includes any files submitted by the user and proctoring information collected by our bot during the assessment. Dedicated storage services are deployed for different types of secondary data based on function and format.

Chat databases

Primary information about the chat is stored in a MySQL-backed database service and is sharded and replicated as needed to meet performance and high availability requirements. The stored assessment information is used to score the candidates' performance and report to the recruiters in real-time.

Organization databases

Organization information required for access management, storing purchased assessments, and administering the assessments are stored in a MySQL-backed database service and are sharded and replicated as needed to meet performance and high availability requirements.

Secondary app servers

Adaface secondary app servers are responsible for scheduling and running automated tasks and notifications. These sub-services are responsible for automating recruiters' workflow and are customizable. Automated tasks include monitoring conversational assessments and ending the unended sessions. They also take care of canceling unused invites so that recruiters can claim the credits and use them for more invites. Our dedicated notification sub-services are responsible for alerting recruiters and candidates via emails. This includes sending reminder emails for inactive candidates and custom test request email notifications.

Primary app servers

Adaface Primary app servers are built to automatically scale based on recruiters' usage. They handle the logic, data processing, and data synchronization of all organization data. They are responsible for authentication, customization, and accessing entire organization data. Security is built into multiple layers of our app servers ensuring that every action is logged and served only based on a user's roles and permissions.

Infrastructure: Behind the scenes

Our engineering team works continuously to innovate and implement secure practices in every layer of our applications. Here are some common segments:

Data centers

Adaface production systems are housed at third-party subservice organization data centers and managed service providers located in the United States. These third-party service providers are responsible for the physical, environmental, and operational security controls at the boundaries of Adaface infrastructure. Adaface is responsible for the logical, network, and application security of our infrastructure housed at third-party data centers.

Encryption

Adaface data at rest is encrypted using 256-bit Advanced Encryption Standard (AES). To protect data in transit between apps (currently API, or web) and our servers, Adaface uses Secure Sockets Layer (SSL)/Transport Layer Security (TLS) for data transfer, creating a secure tunnel protected by 128-bit or higher Advanced Encryption Standard (AES) encryption. Similarly, data in transit between an Adaface client (API, or web) and the hosted services is encrypted via SSL/TLS.

Certificate pinning

Adaface does certificate pinning in modern browsers that support the HTTP Public Key Pinning specification in most scenarios and implementations. Certificate pinning is an extra check to make sure that the service you’re connecting to is really who they say they are and not an imposter. We use it to guard against other ways that skilled hackers may try to spy on your activity.

Perfect forward secrecy

For endpoints we control and modern browsers, we use strong ciphers and support perfect forward secrecy. By implementing perfect forward secrecy, we've made it so our private SSL key can't be used to decrypt past Internet traffic. This adds extra protection to encrypted communications with Adaface, essentially disconnecting each session from all previous sessions. Additionally, on the web, we flag all authentication cookies as secure and enable HTTP Strict Transport Security (HSTS).

Key management

Adaface's key management infrastructure is designed with operational, technical, and procedural security controls with very limited direct access to keys. Encryption key generation, exchange, and storage are distributed for decentralized processing.

Adaface Compliance

Adaface is a secure, safe, and effective platform for enterprises that meets global compliance standards on data, privacy, and protection.

Take the guesswork out of corporate compliance obligations

Adaface meets global regulatory standards for many of your data handling needs. Learn more about the details in our security whitepaper and rest assured that important data is stored securely within Adaface infrastructure.

Learn more about cookie policy

Count on stringent cloud compliance standards and regulations

Your company's compliance issues, standards, and regulations are unique. Adaface combines accepted standards with compliance risk assessment measures geared to the specific needs of our customers' corporate policies, businesses, or industries.

Learn more about GDPR

Check common GDPR FAQs

The best regulatory compliance efforts adhere to a global standard

We test the risk areas of our systems and controls against some of the most widely-accepted security standards in the world. This includes internal and external application security testing and penetration testing.

Cookie Policy

At Adaface, we believe in being transparent about how we collect and use data. This policy provides information about how and when we use cookies for these purposes. Capitalised terms used in this policy but not defined have the meaning set out in our Privacy policy, which also includes additional details about the collection and use of information at Adaface.

What is a cookie?

Cookies are small text files sent by us to your computer or mobile device which enable Adaface features and functionality. They are unique to your account or your browser. Session-based cookies last only while your browser is open and are automatically deleted when you close your browser. Persistent cookies last until you or your browser delete them or until they expire.

Does Adaface use cookies?

Yes. Adaface uses cookies and similar technologies such as single-pixel gifs and web beacons. We use both session-based and persistent cookies. Adaface sets and accesses our own cookies on the domains operated by Adaface. We also use third-party cookies such as Google Analytics.

How does Adaface use cookies?

Some cookies are associated with your account and personal information in order to remember that you are logged in and which dashboards you are logged in to. Other cookies are not linked to your account; these cookies are unique and allow us to perform analytics and customisation, among other actions.

Cookies can be used to recognise you when you visit our sites/ services, remember your preferences and give you a personalised experience that is consistent with your settings. Cookies also make your interactions faster and more secure. Here's the categorization of our usage of cookies:

Authentication: If you've signed in to Adaface, cookies help us show you the right information and personalise your experience.

Security: We use cookies to enable and support our security features, and also to help us detect malicious activity.

Preferences, features and services: Cookies can tell us which language you prefer and your communication preferences. They can help you complete forms on our sites more easily. They also provide you with features, insights and customised content.

Marketing: We may use cookies to help us deliver marketing campaigns and track their performance (e.g. a user visited our Questions pages and then made a purchase).

Performance, analytics and research: Cookies help us learn how well our site and dashboard perform. We also use cookies to understand, improve and research products, features and services, including to create logs and record when you access Adaface from different devices.

Are cookies used for advertising purposes?

No. Adaface does not serve any advertisements.

What can you do if you don't want cookies to be set or want them removed?

Some people prefer not to allow cookies, which is why most browsers give you the ability to manage cookies to suit you. In some browsers, you can set up rules to manage cookies on a site-by-site basis, giving you more nuanced control over your privacy. What this means is that you can disallow cookies from all sites except those that you trust. Browser manufacturers provide help pages relating to cookie management in their products. Please see below for more information.

- Google Chrome
- Internet Explorer
- Mozilla Firefox
- Safari (desktop)
- Safari (mobile)
- Android Browser
- Opera
- Opera Mobile

For other browsers, please consult the documentation provided by your browser manufacturer.

Note that if you limit the ability of websites and applications to set cookies, you may worsen your overall user experience and/or lose the ability to access the services because they will no longer be personalised to you. Doing this may also stop you from saving custom settings, such as login information.

Does Adaface respond to "do not track" signals?

Adaface does not collect personal information about your online activities over time and across third-party websites or online services. As a consequence, "do not track" signals transmitted from web browsers do not apply to Adaface and we do not alter any of our data collection and use practices if we receive such a signal.

Adaface's GDPR Commitment

We are committed to honoring our users' rights to data privacy and protection. Even if our users might not be based in the EU, their candidates may be, so it is important that Adaface become GDPR compliant to ensure all our clients are covered. We have implemented technical and organizational measures to be fully compliant with GDPR.

Data processing and ownership

During the course of recruiting, our clients need to collect PII (Personally Identifiable Information) from candidates to build a profile and perform an automated evaluation using our assessment chatbot.

When a candidate begins an assessment session initiated by an Adaface client, we store the following information of the candidate on behalf of our client:

- Email address
- Name
- Optional at the client's discretion: Phone number, the last school attended, academic degree, major, programming experience, resume, and a link to social profiles (GitHub, LinkedIn, etc).

If the recruiter uses an Adaface account for inviting candidates to assessments, we store the following information:

- Name
- Email address
- Phone number (Optional)

This data comes under the purview of GDPR. Given that the processing should be fair, Adaface ensures that we obtain consent from candidates when they sign up (using their invited emails to access our assessments). Our updated privacy policy clearly states how we process information in a fair and transparent manner. All the candidate information we receive or collect is handled securely with adequate data protection.

Data Subject Rights

Under GDPR, individuals have the right to ask the organizations they apply to for the right to portability, rectify and be forgotten. Adaface collects candidates' data on behalf of our clients, any requests regarding accessing/ editing/ deleting of candidates' data will be forwarded to our clients. We give our clients the mechanisms to access their candidates' data and also comply with requests from their candidates. This way, our customers are always in control of their candidate data.

Our client can determine if the candidate's request is valid and can be fulfilled. We will take action based on the direction provided by our client on how to proceed with any such request.

As a processor, Adaface gives flexibility to our clients to determine their data policies, which offer rights to their candidates. This includes the ability to access / edit/ delete information regarding a candidate. We also give the ability to set a routine data deletion process at a cadence determined by the client.

Data Management

Data within Adaface is secured using industry-standard encryption. Data can be transferred outside EU borders if our client and Adaface have entered into a contract that includes contractual clauses specified by EU. Adaface has a standard EU-specific data transfer and processing agreement to ensure compliance with GDPR.

GDPR also stipulates that personally identifiable data should not be stored indefinitely. Adaface's data retention policy provides flexibility to our client to define how long their candidates' PII should be stored and when it should be deleted. Data is stored for the duration of the contracted period with our client, and a grace period thereafter.

Adaface maintains a detailed audit log of all the activities. As part of compliance, Adaface will add any additional activities that our clients need to be recorded. These logs are viewable in our dashboard or can be requested for export/ deletion by contacting us at ada@adaface.com.

Data Breach and Mitigation Process

We have sufficient data monitoring mechanisms in place to become aware of any data breach. In case a personal data breach occurs, we will send breach notifications in accordance with our internal incident response policy (within 72 hours of us discovering the breach). This will give sufficient time for our clients to convey the breach to the respective authorities. Additionally, we will notify users through our blogs and social media for general incidents. We will notify the concerned party through email (using the primary email address) for incidents specific to an individual user or an organization.

Our security infrastructure standards

Protecting our customers' information and their users' and candidates' privacy is extremely important to us. As a cloud-based company entrusted with some of our customers' most valuable data, we've set high standards for security.

Adaface has invested heavily in building a robust security team, one that can handle a variety of issues – everything from threat detection to building new tools. In accordance with GDPR requirements relating to security incident notifications, Adaface will continue to meet its obligations and offer contractual assurances.

If you'd like to learn more about Adaface's security policies and procedures, please see our security page. It provides detailed information on how we approach security, and includes a white paper on how Adaface ensures user data security in particular, including our technical and organisational measures(TOMs), as well as our encryption standards.

Updates

At Adaface, we are committed to the security and privacy of your data. So we're glad to comply, and help you to comply with the GDPR. If you have any questions about your rights under the GDPR as a user, or how Adaface can help you with compliance as a customer, we hope that you'll get in touch with us at ada@adaface.com. Please also visit our Trust Guide to learn more about our privacy, security and compliance programmes.

Resources

- Adaface GDPR FAQs
- Privacy Policy
- Security Whitepaper
- Security
- EU-US Privacy Shield and Swiss-US Privacy Shield
- Full text of the GDPR

Adaface GDPR FAQs

Adaface is committed to adhering to the General Data Protection Regulation (GDPR) policies. The following are some of the frequently asked questions to help our clients and candidates.

Clients/ Organizations/ Users with an Adaface account

What data do we collect?

When a candidate begins an assessment session initiated by an Adaface client, we store the following information of the candidate on behalf of our client:

- Email address
- Name
- Optional at the client's discretion: Phone number, The last school attended, academic degree, major, programming experience, resume, and a link to social profiles (GitHub, LinkedIn, etc).

If the recruiter uses an Adaface account for inviting candidates to assessments, we store the following information:

- Name
- Email address
- Phone number (Optional)

Who is responsible for candidate data?

Any Adaface client that administers the assessment owns the data of all candidates that took the assessment. The responsibility of updating and deleting all candidate data when requested by a candidate lies with the client. Adaface provides our clients with necessary support (customer support/ product features) to carry out any such requests however the company wants to.

For how long is the candidate data stored?

It depends on the contract with our client. By default, we store data until it's explicitly removed. But we provide provisions to set up a periodic data removal process for our clients on a contract-to-contract basis. However, we always support data deletion through requests sent to ada@adaface.com for all of our clients. We delete data at the specified/ requested time by our clients with an additional grace period.

Who has access to candidate data?

- Clients that administer the assessment.
- Candidate through requests to Client.
- Adaface internal team only when a support request is raised by the Client and data access is necessary to support such request.

Which roles/ permissions are required for employees of the client to have access to candidate data?

All users of a client account with roles - Candidates Admin, Tests Admin, Super Admin have access to candidate reports.

How do clients request candidate data to be deleted?

For enterprise users with specific contracts, they can delete the candidate entry using 'delete' action in candidates' view. Furthermore, you can email us at ada@adaface.com with the list of candidates' data to be deleted. You can also contact your Adaface Customer Success Manager for such requests.

How to access audit logs?

Adaface maintains logs of all actions that are state changing as well as unpermissioned actions for troubleshooting and security. Super Admins of a client account can view the audit logs from their dashboard. Any further processing requests of audit logs should be routed through ada@adaface.com or your Adaface Customer Success Manager.

Can the deleted data be reinstated?

No.

Can we edit a candidate's data?

For editing a candidate's data, please contact us at ada@adaface.com with details about the request.

Candidates who took the Adaface technical chat

Can I delete/ edit/ view/ access my test attempt or personal information?

Adaface is an assessment provider and the data of the technical chat including the scorecard is owned by our client who administered the assessment. Please contact the client who administered the assessment directly to request the deletion of your data. If you require any help in making such requests, you can contact us at ada@adaface.com.

Security Practices

External and internal application security testing

Our security team performs automated and manual application security testing on a regular basis to identify and patch potential security vulnerabilities and bugs on our applications.

Internal audits

We audit our systems and controls against some of the most widely-accepted security standards and regulations in the world. These reviews occur at least annually and are thorough in their inspections.

Continual improvement

A critical part of any information security management program is the continual improvement of security programs, systems, and controls. To this end, Adaface is committed to soliciting feedback from different internal teams, customers, internal and external auditors, and using this feedback to develop improved processes and controls.

Data management: transparency and control

This resource provides insight into Adaface's data management policies and practices, as well as information about the tools that you need to manage, protect and control your data.

Who is responsible for candidate data?

Any Adaface client that administers the assessment owns the data of all candidates that took the assessment. The responsibility of updating and deleting all candidate data when requested by a candidate lies with the client. Adaface provides our clients with necessary support (customer support/ product features) to carry out any such requests however the company wants to.

What data portability tools are available with Adaface, and who can use them?

What data customers may access using Adaface's import and export tools are specific to each subscription, but we have given an overview below.

On any plan, super admins can export all candidate data from Adaface dashboard. Super admins can request self-service export functionality required for their organization's policies. Please note that all requests are subject to an application process to ensure that (a) appropriate employment agreements and corporate policies have been implemented, and (b) all use of data exports is permitted under applicable law.

Additionally, Integrations APIs allow eligible Adaface customers to use third-party applications to export, retain or archive candidate's data submitted to Adaface.

How to access audit logs?

Adaface maintains logs of all actions that are state changing as well as unpermissioned actions for troubleshooting and security. Super admins of a client account can view the audit logs from their dashboard. Any further processing requests of audit logs should be routed through ada@adaface.com or your Adaface Customer Success Manager.

How do we use information to improve Adaface?

We analyse aggregated and disassociated Customer Data that is submitted to Adaface, as well as Other Information, to find patterns that help us to make our customers' experiences better.

For example, we may improve our ready-to-go test library based on popular skills requested and used by our clients. We might also use test usage information to prioritize our test library.

Where is your data stored?

Adaface is hosted with Digital Ocean. The default data centre is in the United States, but some customers may choose to use our data residency capability. Data residency for Adaface allows global teams to choose the region or country where their data is stored at rest.

Data Residency for Adaface

Some Adaface customers (as per their agreement with Adaface) are now able to choose which country or region their data is stored in while fulfilling corporate policies and compliance requirements

In the not too distant past, when on-premises software was the norm, data storage was simple. Your data lived with you. Today, cloud services make data residency more complicated. Global organisations are creating their own internal policies for where data can be stored, while governments and third-party regulators are enforcing data residency requirements.

Enterprises around the world collaborate in Adaface each day for their screening requirements, but because data is primarily stored in the United States, many teams abroad remain on the sidelines. To bridge this gap – and make Adaface available to more teams in highly regulated sectors, such as financial services, the public sector and healthcare – we're delivering data residency for Adaface.

Data residency gives global teams more control over where their data is stored. Data regions currently available outside the US include:

- United States
- Netherlands
- Singapore
- United Kingdom
- Germany
- Canada
- India

With data residency, what type of data does Adaface store?

Candidate chat history, assessment data and performance information is stored at rest within a desired data region.

I'm an existing customer. Can I move my data to a new region?

Yes. Speak with your Adaface account manager on the additional charges or plan changes that are required for moving to new residency regions.

If I move my data to a new region, will anything else change?

No. Everything remains the same for the recruiters and candidates.

Conclusion

We have an existential interest in protecting your data. Every person, team, and organization deserves and expects their data to be secure and confidential. Safeguarding this data is a critical responsibility we have to our customers, and we continue to work hard to maintain that trust. Please contact your account manager if you have any questions or concerns.