Company-Wide Security Policy

Version 2.0

Last updated on November 12, 2018

Table of Contents

Contents

Pinsight® is a talent assessment company operating on a cloud-based platform.

Full Legal Name: Global Assessor Pool LLC dba Pinsight®
Company Type: LLC
State of Incorporation: Colorado
Address: PO Box 18576 Denver CO 80218 USA
Phone Number: 800-423-8295
Physical Address: 550 E. 12th Avenue, #609 Denver CO 80203 USA

This document outlines Pinsight®'s technology platform and its company-wide program related to cybersecurity. All Pinsight® employees and contractors are required to complete security training and certify that they comply with standards set forth in this document.

1. Background

Since 2010, we have completed thousands of talent assessments with our technology platform in 30 countries and in 8 languages. There are over 100 companies in every industry using our technology to deliver employee assessment and development programs. We were the Gold winner in 2015 in the Simulation and Gaming category awarded by the Chief Learning Officer magazine and we were the Silver winner in 2016 in the Best Use of Games or Simulations for Learning category awarded by Brandon Hall Group. In April 2018, we released an updated technology platform featuring the Leader Habit app.

Pinsight® has consultants all over the world who help to successfully execute projects. Our core team has PhD and Master's level employees as well as highly-qualified technical and support staff.

Pinsight®'s Leader Readiness Platform (our core technology platform) offers an integrated leadership development and virtual simulation assessment platform (aka. assessment centers). We follow the assessment center guidelines put forth by the International Taskforce on Assessment Center Method in developing and administering assessment centers. Additionally, we follow International Test Commission's guidelines on online testing.

2. Privacy and Collection

Pinsight® collects the following personal information from users of the Leader Readiness Platform: name, email, telephone number, location (city, state). This information is collected directly from the users when they are completing their user profile. Simulation participants have the option of providing additional information about themselves for EEO and research purposes including their age, race, gender, years of work experience, educational status, company industry and level in the organization. This information is entirely voluntary, and participants are not required to report this. During a simulation, participants create email messages, notes, video voicemail messages and calendar events related to the fictitious simulation scenario. Also, participants engage in interactive video conversations that are recorded and saved to our servers.

Pinsight® uses subcontractors to act as role-players and raters during the simulation assessments. They perform live video role plays with the participants, and also have access to all the emails, recorded video voicemails, and video role-plays the participant completes so they are able to conduct the ratings on the leadership skills of the participant. All of these responses are considered fictitious in nature as they are responses to simulated events.

Pinsight users directly interact with the Leader Readiness Platform. The platform is branded with the company logo. Users can view their personal information and can modify their user profile and reset their password by logging into app.pinsight.com. Users are not able to delete their information; however, they can contact Pinsight directly to delete or deactivate their account.

Pinsight® is subject to regulatory requirements by EU data privacy. All personal information is stored in the United States. Pinsight® participates in the EU-US Privacy Shield.

3. Information Security

Data is stored in MySQL 5 version 5.5.59 databases. We utilize classic LINUX servers that utilize Long Time Support (LTS) versions, meaning periodic updates occur on our servers. Our tools are developed in common and generally accepted web-based technologies and languages such as, PHP (Symfony), HTML, CSS, JavaScript (React), and AJAX.

Our servers are, in part, hosted in Tier 3 data centers with backup power generators. Code and data is backed up to DigitalOcean.

Our servers are set up with firewalls, regular antivirus scans, and regular database backups. Our database backups utilize Amazon S3 and Digital Ocean servers to be backed-up in at least two different geographic locations. Web-based applications utilize secure access to directories, thus preventing unauthorized access. Access to the frontend (i.e., portion that candidates see) is secured by user-generated passwords that require strong criteria (at least 8 characters, one uppercase letter, one number and special character). Passwords are protected by using Bcrypt. All communication between our servers and client/candidate runs through secured HTTPS connection using SSL certificate.

Pinsight® runs on a Virtual Private Server (VPS). A VPS runs its own copy of an operating system, and we have superuser-level access to that operating system instance, so we can install almost any software that runs on that OS. VPS is functionally equivalent to a dedicated physical server. We share the underlying physical hardware with other VPSs.
A VPS which is dynamic (that is, it can be changed at runtime) is often referred to as a cloud server. Key attributes for this are:

- Additional hardware resources can be added at runtime (CPU, RAM)
- Server can be moved to other hardware while the server is running (automatically according to load in some cases)

Our VPS characteristics:

- 8 GB RAM DDR3 and 80 GB disc space
- shared processor (Intel Xeon E5-2630L 2 GHz – 4 threads)
- possibility to change the configuration without data loss
- customizable administrator interface
- full administrative (root) access
- preinstalled operational system - Ubuntu
- unlimited data transfer, 1Gbps connection of availability 99,99%
- weekly backups
- 1 fixed public IPv4 address

SSL Certificates are small data files that digitally bind a cryptographic key to an organization's details. When installed on a web server, it activates the padlock and the https protocol (over port 443) and allows secure connections from a web server to a browser. Typically, SSL is used to secure data transfer and logins, and more recently is becoming the industry standard.

Pinsight® utilizes a Wildcard SSL certificate. The technical specifications are: Standard X.509 certificates, Symmetric 256-bit encryption, RSA public-key SHA-2 algorithm (supports hash functions: 256, 384, 512), ECC public-key cryptography (supports hash functions: 256 and 384), Unlimited server licensing, Supports 2048-bit public key encryption (3072-bit and 4096-bit available). SSL reports for pinsight.com can be found at: https://www.ssllabs.com/ssltest/analyze.html?d=pinsight.com) and SSL reports for app.pinsight.com can be found at: https://www.ssllabs.com/ssltest/analyze.html?d=app.pinsight.com

Pinsight uses AES256. AES is based on a design principle known as a substitution–permutation network and is efficient in both software and hardware. Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. By contrast, Rijndael per se is specified with block and key sizes that may be any multiple of 32 bits, with a minimum of 128 and a maximum of 256 bits.

AES operates on a 4 × 4 column-major order matrix of bytes, termed the state, although some versions of Rijndael have a larger block size and have additional columns in the state. Most AES calculations are done in a special finite field.

Pinsight® is optimized to handle multiple users being in the system at one single moment. Pinsight®'s security policy is communicated through this document, employee handbook, and training. All of relevant parties must certify compliance with our security policy. Our security policy is approved by management, reviewed annually, legally binding and covers the following:

- Code of conduct
- Account management

- Passwords
- Third party information security
- Email appropriate use

Pinsight® ensures assessment security by conducting periodic scans of the Internet to determine if there are any discussions, posts and/or pictures that would give an unfair advantage to participants.

Apart from Digital Ocean backups, we do our own backups. We back up databases, config files for server, frontend and backend. We use a scheme called grandfather-father-son backup (https://www.handybackup.net/grandfather-father-son-backup.shtml). Backups are saved to Amazon S3 Bucket where everything is encrypted (AES256) with a different key from the one we are using to encrypt data in DB alone).

PDF reports, participants files from simulations, pictures/avatars are backed up through synchronization to Amazon S3 as well (live sync) - encrypted by AES256.

Role-plays and voicemails are saved to Amazon S3 from tokbox directly. Access to them is limited – they are not publicly available and for user to have access – s/he needs to be logged in to our system and have neccessary permissions to view (for example – assessors can see only those recordings for whom they were assigned).

4. Organization of information security

Our IT manager has overall responsibility for information security. The IT manager, employees, contractors and all relevant parties are required to sign a confidentiality agreement. Pinsight®'s solution allows data to leave the boundaries of the United States to the European Union.

5. Asset management

Pinsight® maintains an inventory of all assets and all information assets have a designated owner.

Asset	Data	Role	People
Amazon	Storage	Admin	IT manager
Gitlab (selfhosted)	Source code manager	Admin	IT manager
Gitlab (selfhosted)	Continuous integration and delivery service	Admin	IT manager
Digicert	SSL certificate	Admin	It manager Office manager
Digital Ocean	Server	Admin	IT manager
Google Apps for Business	Google Drive Gmail	Super Admin	Office manager

Google Apps for Business	Google Drive Gmail	Users	Employees, certain contractors and partners
LastPass	Passwords	Admin	Office manager
Microsoft 365	OneDrive Email	Admin	Office manager IT manager
Microsoft 365	OneDrive Email	Users	Employees
Pinsight	Simulator.pinsight.biz	Super Admin	Certain employees and contractors
Pinsight	app@pinsight.com	Admins and users	Employees, contractors, partners, clients, stakeholders and participants
Prey Project	Company laptops	Admin	Certain employees
Prey Project	Company laptops	Users	Certain employees
RapidSSL	Security certificate	Admin	IT manager
Slack	Communication and file sharing	Admin	IT manager
Stripe	Payment processing	Admin	Office Manager
TokBox	Video conferencing	Admin	IT manager Office Manager
Trello	Project management software	Admin	IT manager
Wedos	Database	Admin	IT Manager
Zoho One	Tech support chats, CRM, email campaigns	Admin	Office manager
Serverdensity	Server monitoring	Admin	IT manager

6. Human resources security

Pinsight® obtains signed agreements from all employees and contractors that states adherence to the security policy. Pinsight® conducts background checks on employees who have access to financial data. Verification of previous employment and references are conducted for all employees. All employees receive security awareness training as part of the onboarding process. When employees, contractors, and all relevant parties are terminated, they are promptly removed from having any access to information assets. They are required to immediately return company-owned equipment and physical materials.

7. Physical and environmental security

Pinsight utilizes data centers including servers hosted with AmazonS3 and Digital Ocean. AWS performs initial environmental and geographic assessments. Data center locations are carefully selected to mitigate environmental risks, such as flooding, extreme weather, and seismic activity. AWS Availability Zones are built to be independent and physically separated from one another.

AWS data centers are designed to anticipate and tolerate failure while maintaining service levels. In case of failure, automated processes move traffic away from the affected area. Core applications are deployed to an N+1 standard, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.

AWS has identified critical system components required to maintain the availability of our system and recover service in the event of outage. Critical system components are backed up across multiple, isolated locations known as Availability Zones. Each Availability Zone is engineered to operate independently with high reliability. Availability Zones are connected to enable you to easily architect applications that automatically fail-over between Availability Zones without interruption. Highly resilient systems, and therefore service availability, is a function of the system design. Through the use of Availability Zones and data replication, AWS customers can achieve extremely short recovery time and recovery point objectives, as well as the highest levels of service availability. More information is available at: https://aws.amazon.com/compliance/data-center/controls/

Digital Ocean datacenters are co-located in some of the most respected datacenter facility providers in the world. Digital Ocean leverages all of the capabilities of these providers including physical security and environmental controls to secure their infrastructure from physical threat or impact. Each site is staffed 24/7/365 with on-site physical security to protect against unauthorized entry. Security controls provided by our datacenter facilities includes but is not limited to:

- 24/7 Physical security guard services
- Physical entry restrictions to the property and the facility
- Physical entry restrictions to our co-located datacenter within the facility
- Full CCTV coverage externally and internally for the facility
- Biometric readers with two-factor authentication
- Facilities are unmarked as to not draw attention from the outside
- Battery and generator backup
- Generator fuel carrier redundancy
- Secure loading zones for delivery of equipment

For more information on Digital Ocean's physical security, please visit: https://www.digitalocean.com/security/

8. Communications and operations management

Pinsight®'s documented change process includes using version control on Gitlab. We have physically and logically separated environments for development, testing, and operations. Pinsight® has policies in place to protect against viruses, worms, and spyware. Desktop and server antivirus signatures are updated daily. The process to identify and promptly distribute security patches is done on daily basis. Pinsight® is separated from the internet by a firewall. All company computers for full-time employees are protected with Windows firewall with

recommended settings and automatic updates. The company's web servers, application servers, and databases are logically separated based on participant ID.

Remote access is controlled for employees by using server side logs + user management within Google Apps for Business and Microsoft Office 365. Controls for third party suppliers are not used because they are not permitted. Data is not physically segregated in order to properly identify and control access to data from separate customers and there are not dedicated systems for each client.

The network and host-based IDS is deployed on all internet connections, servers and work stations that are utilized by our full-time employees. For our contractors, this would be dependent on each of their internet service providers.
Pinsight® retains audit logs of user activity for 6 months and keeps and reviews logs of System Administrator for 6 months as well. The transfer of personal information is encrypted using an SSL certificate, AES 256 CBC // HMAC - SHA1 for message authentication // DHE - RSA for key exchange mechanism. Pinsight®'s data is not stored on any devices such as, USB, CD/DVD, laptop computers, PDAs, tablets, smart phones, or backup tapes. Data is backed up every 24 hours and stored offsite.

9. Access control

The formal process for approving/granting access involves employees and contractors reviewing and signing our employment or service provider contract, as well as submitting all necessarily new-hire paperwork which can include a background check screening, before they are granted access. Both, the employment and service provider contracts include information about the security policies and confidentiality of data.

Upon termination of the employment or service provider contract, access is immediately denied by deactivating login information associated with that employee or contractor. They have a single login to access the Pinsight platform, so this is quickly and promptly done when employment is terminated.

Contractors all receive the same privileges which includes access to the data only directly relating to individuals they have been assigned to work with. No contractor has full access to all the data, only Pinsight® admin accounts have this ability.

Each user has a unique, non-generic login ID. Users are granted minimum access based on the role of their job. Contractors and clients are granted access only to the data that directly pertains to the candidates they are working with. No users other than Pinsight® admin have access to all the data. Encrypted VPNs are used for all remote access to internal systems. FTP and SSL are the mechanisms used for the authentication process for remote access.

Staff computers use screen savers after equipment is left unattended for 15 minutes.

10. Information systems acquisition, development, and maintenance

Pinsight® develops its own applications/software to deliver its services online. There are controls in place to prevent unauthorized modification of source code. Live data or personal information is prohibited from being used in test environments. User access is protected using SSL encryption. User accounts are immediately deleted when no longer needed.
Pinsight® passwords for contractors, clients, and candidates are user-generated and require strong criteria of at least 8 characters. Contractors, clients, and candidates are able to reset their password by clicking on the Forgot Password link, at which time they will receive an email notification with instructions to click a link to create their new, secure password. The link expires one hour after delivery or after it has been used once. Passwords are protected using Bcrypt.

For encryption at rest we are using synchronous AES (https://dev.mysql.com/doc/refman/5.5/en/encryption-functions.html) which means that in case of a breach – data is encrypted and would need to be decrypted to gain any value out of it (the key is 32 characters long and saved directly on the server).

Passwords for company laptops are changed every 90 days and previously used passwords are not allowed.

Controls are in place to prevent other clients from accessing Pinsight® data by the data being separated by client in the backend of the database, as well as in the front end of the user interface. Access is restricted for each client to only participants they have entered. Client access is password hashed using Bcrypt.

Pinsight®'s application uses role-based user access based on permissions hierarchy, which includes:, Admin, Partner Owner, Partner Admin, Client Owner, Client Admin, Assessors, Participants, Stakeholders. For instance, admins only have access to information relevant to their role and they do not see information of other partners. Also, participants and stakeholders only see what is relevant to them and what has been shared with them. Assessors are only able to see report information of those participant simulations that they were involved in. Lastly, PDF reports utilize privacy by design, meaning that only users who have been shared permissions can access this information.

Pinsight®'s website uses session-based cookies. The cookies are managed by a PHP module and contain a session ID.

11. Information security incident management

We are monitoring our servers via a third party – Serverdensity. We monitor these parameters:

1. application availability based on 3 different geographical locations
2. API availability based on 3 different geographical locations
3. server state – on/off/load – in case of a problem we receive alerts
4. amount of free RAM – if less than 10% we receive alerts

5. amount of free HDD – if more than 80% we receive alert

Pinsight® has not had loss of equipment or data, but if an incident were to happen, we would launch a formal investigation immediately. If a security breach occurred, we would notify our clients within 24-48 hours by phone and by written communication via email. We would immediately make reasonable efforts to prevent further loss of data and to control an existing situation. We will report more details of the situation as more information becomes available. For those Pinsight users who are citizens of the EU, we would also report the breach to the relevant GDPR data protection supervisory authority within 72 hours of the security breach. (Listing of DPA's)

Pinsight® installs Prey Project on all company laptops. Prey Project is an anti-theft protection software that monitors company computer locations and helps recover them if lost or stolen. After installing the software, Prey runs in the background and can be activated by an administrator as needed. Once remotely triggered, the device will gather and deliver detailed information of who is using the device. Prey allows for remote lock down of devices and to delete stored passwords.

Pinsight® utilizes LastPass Enterprise to protect all company passwords. LastPass Enterprise offers employees and admins a single, unified experience that combines the power of SAML SSO coupled with enterprise-class password vaulting. LastPass protects our digital assets from the risks associated with employee password re-use and phishing. LastPass Shared Folders allow administrators to easily share credentials for a single website or for a group of sites while retaining the ability to tie activity back to the individual user. Password updates automatically and seamlessly propagate to all assigned users eliminating lock-out caused by version control issues.

In its default state, LastPass Administrators cannot access any data stored in an employee's LastPass account. However, there are some exceptions: (1) the end user can explicitly share data with an Administrator via an individual share or a Shared Folder, or (2) the company can choose to enable either or both of the Super Admin Policies defined here: https://lastpass.com/policy_doc.php. When the Super Admin Policies are enabled, a notification is sent automatically to every LastPass Admin in the Enterprise.

Employee accounts can be instantly disabled when employees leave the organization and administrators can view historical data and can audit employee logins and accesses. LastPass uses multifactor authentication offering increased security. Using an evolved host-proof hosted solution, LastPass employs localized, government-level encryption (256-bit AES implemented in C++ and JavaScript) and local one-way salted hashes to provide complete security with the convenience of syncing through the cloud. All encrypting and decrypting happens on individual computers – no one at LastPass can ever access sensitive corporate data. The LastPass™ Security Challenge also allows users to identify weak account data and provides suggestions for significantly improving online security.

We use a ticketing system from Zoho Support, which allows for various state of tickets of level 1 and level 2 support. This provides immediate support to simulation participants and clients alike.

12. Business continuity management

In the event of disruption, Pinsight® has an emergency notification process where the appropriate contacts receive communication that service is out and should be restored in the least amount of time possible. We notify vendors and customers in the event of a service outage.

13. Compliance

Pinsight®'s security policy is compliant with data protection and privacy requirements. Pinsight® is responsible for the following:

- Application software development
- Application end-user support
- Database administration
- Software testing and acceptance
- Software upgrades
- User account administration
- Application security policies including password and lockout policy
- Infrastructure management
- Data backup and restore
- Operating System security vulnerability patching
- Application security vulnerability patching
- Operating System anti-malware protection and updates
- Platform change management
- Firewall and network access management
- Platform activity log review
- Incident management, detection, recording, response
- Application availability and performance monitoring
- Network vulnerability scans and/or penetration testing
- Application vulnerability scans and/or penetration testing
- Secure data destruction, data from damaged or obsolete storage devices, retired servers

14. Appendix A: Privacy Policy

1. What this policy covers

GLOBAL ASSESSOR POOL, LLC, dba Pinsight® ("Company" or "we" or "us") is committed to protecting your privacy. We prepared this Privacy Policy to describe our practices regarding the information we collect from users of our websites, located at http://www.pinsight.com, https://www.leaderhabit.com/, https://app.pinsight.com/, and use of our related services (including any web or mobile applications).

2. Information we collect

We collect information directly from you, when you access our websites and related services, from 3rd parties, and automatically when you access our websites and platform.

Information you give us

We collect information from you when you become a Pinsight user as an account owner or admin, as an assessor, as a stakeholder, or as a participant in the Leader Readiness Platform and/or the Leader Habit app. We collect this information when you create or change your profile information including your contact information, time zone, profile picture, and your notification preferences.

We collect information you provide to us when you enroll in a webinar, request a demo, participate in an online chat, subscribe to our newsletter, or take the Leader Habit Quiz. For example, when you request a demo, we must have your contact information, so we can contact you to schedule the demo. When you take the Leader Habit Quiz, we collect your responses to a set of questions that comprise the quiz and we collect your email address, so we can deliver your report.

Information collected when you use our services

When you use the Leader Readiness Platform, we record all of the actions you take. If you are an administrator, we record who you invite to assessments and who you share reports with. If you are participating in a Pinsight assessment as an assessor, we record any role-plays you participate in, the scores you assign, and when you log in and out of the platform. If you are participating in a Pinsight assessment as a participant, we collect and store all of the emails and file attachments that you send during the pre-work stage and the live simulation. We also record and save voice mail messages you leave, calendar appointments you make, and online chats and role-plays you participate in. Trained assessors use this information to score your performance on a variety of exercises. These scores are recorded and used to create a report on your performance. If you have access to the Leader Habit App, we record usage data, for example, when you log into your account, when you complete an exercise, comments you enter, and improvement over time.

Information collected from others

We may receive information about you from others. For example, if you are participating in an assessment at the request of one of our clients, we may receive your contact information from our

client so that we can invite you to become a Pinsight user. After accepting an invitation, you will be able to update your profile and make changes to your personal information.

We may also collect data from companies contracted by us to provide add-on services to our platform. We currently contract with "cut-e" an Aon company that provides one of the components of our assessments. If you participate in one of our assessments, you will complete a learning efficiency test. After completing the learning efficiency test, cut-e provides Pinsight with the results of your test using an anonymous numerical identifier generated by Pinsight. For more information about cut-e visit https://www.cut-e.com/assessment-solutions/

Information Collected automatically via your devices and browsers

To make our website and related services more useful to you, our servers (which may be hosted by a third-party service provider) collect information about the devices and computers you use to access our website and services. This includes browser type, operating system, Internet Protocol (IP) address, domain name, and/or the date and time of your visit. We also use Cookies and navigational data to gather information regarding the date and time and duration of your visit, what you searched for, and the pages you viewed. Like most Internet services, we automatically gather this information and store it in log files each time you visit our website or access your account on our network.

What are "Cookies"?

Cookies are small pieces of information that a website sends to your computer's hard drive while you are viewing a web site. We may use both session Cookies (which expire once you close your web browser) and persistent Cookies (which stay on your computer until you delete them) to provide you with a more personal and interactive experience on our website. Persistent Cookies can be removed by following Internet browser help file directions. If you choose to disable Cookies, some areas of our website or service may not work properly.

Analytics

We use Google Analytics and Squarespace Analytics on our websites. Google Analytics and Squarespace Analytics use cookies to help us analyze how you use our website. The information generated by a cookie about your use of the website (including your IP address) is transmitted to and stored by Google and Squarespace on servers in the United States. Both companies use this information to evaluate your use of the site, compile reports on site activity for us, and provide other services relating to site activity and internet usage. This analytics data is not tied to any Personal Information. For more information about Google Analytics, please visit www.google.com/policies/privacy/partners/. For more information about Squarespace Analytics please visit https://support.squarespace.com/hc/en-us/articles/206544167-Squarespace-Analytics-overview

We use Zoho Chat on our website and in the Leader Readiness Platform. Zoho Chat is a live chat app that uses cookies for website visitor tracking. This enables us to identify your location on our site and initiate a conversation with you. For example, if you have a question while taking an assessment, Zoho Chat allows you to ask the question and get a response in real time from a Pinsight employee. For more information about Zoho Chat, please visit https://www.zoho.com/salesiq/

We use TokBox in the Leader Readiness Platform. TokBox is a 3rd party software we use for conducting videocalls. For more information about TokBox, please visit https://tokbox.com/

We currently do not respond to Do Not Track signals.

3. How we use information we collect

We do not sell, trade, share, or rent your personal information to third parties to use for their own marketing purposes. We use the information we collect for the following purposes:

To provide our services and communicate with you

We use your contact information to deliver our services. For example, we use your user name and password to authenticate you when you log in and identify you as a user on our system, we use your contact information to provide customer support, we use your time zone information when scheduling assessments, we use your email address to deliver quiz results and newsletters and depending on your notifications preferences, we send you administrative notifications. We also use your information to inform you of new features or products that we think you would be interested in. You can control marketing communications via the "Unsubscribe" link in an email. You can adjust your user notifications by using your notification preferences in your profile.

We use the data that we collect when you participate in an assessment or use the Leader Habit app to create your Pinsight report. When you participate in an assessment, you complete a learning efficiency test, a personality questionnaire, and a live simulation. The results from these assessments are all used to create your Pinsight report. If you use the Leader Habit app, we track when you enter information and use this information to estimate your improvement.

For research and development

We may create anonymous data records by excluding information (such as your name) that makes the data personally identifiable to you. We use this anonymous data to analyze request and usage patterns to enhance the content of our services and improve site navigation. We may also use anonymous data for research and development purposes, such as scientific articles and presentations, assessor training, and to enhance our services.

To comply with Law

We may use your information to comply with legal obligations, as part of our general business operations, and for other business administration purposes.

4. How we share information

We do not share your personal information except in the following limited circumstances.

We share information with our clients

We share your information with our clients when they engage Pinsight and through our client, you participate in a Pinsight assessment. We disclose assessment information and provide access to your

reports to the client that has engaged us. Information collected during an assessment is maintained in our database. However, downloadable PDF reports may be kept at a client site.

We share information with Pinsight or partner assessors

We share your personal information and assessment information, including recorded role-plays, emails notes, calendar entries, and voice mails with Pinsight assessors or partner assessors who are directly involved in your assessment when you participate in a Pinsight assessment. Sharing this information is essential for assessors to complete scoring assignments and for your assessment report to be generated.

Third Party Links and Websites

We may provide links to other websites or locations for your convenience. This does not signify our endorsement of the website, the location, or its contents. When you choose to click on a link, you will leave our site and go to another site. During this process, another entity may collect information from you. We have no control over, do not review, and cannot be responsible for these outside websites or their content. Please be aware that the terms of this Privacy Policy do not apply to these outside websites or content, or to any collection of data after you click on links to outside websites.

5. Legal basis for processing personal information (EEA residents only)

If you are a resident of the European Economic Area, our legal basis for collecting and using your personal information will depend on the personal information concerned and the specific context in which we collect it.

However, we will normally collect personal information from you only where we have your consent to do so, where we need the personal information to perform a contract with you, or where the processing is in our legitimate interests and not overridden by your data protection interests or fundamental rights and freedoms.

If we ask you to provide personal information to comply to perform a contract with you, we will make this clear at the relevant time and advise you whether the provision of your personal information is mandatory or not (as well as of the possible consequences if you do not provide your personal information). We will also provide you with the option to withdraw consent.

Similarly, if we collect and use your personal information in reliance on our legitimate interests (or those of any third party), we will make clear to you at the relevant time what those legitimate interests are.

If you have questions about or need further information concerning the legal basis on which we collect and use your personal information, please contact us using the contact details provided under "How to contact us".

6. How we store and secure information

We use data hosting service providers in the United States to host the information we collect. We use a variety of industry-standard security technologies and procedures to help protect your information from unauthorized access, use, or disclosure. We may require you to enter a password to access your account information. Please do not disclose your account password to unauthorized people. Despite these measures, you should know that no security system is impenetrable and due to the inherent nature of the Internet, we cannot guarantee that data, during transmission through the Internet or while stored on our systems or otherwise in our care, is absolutely safe from intrusion by others.

7. How long we keep information

We retain personal information we collect from you where we have an ongoing legitimate business need to do so, for example, to provide you with a service you have requested or to comply with applicable legal, tax or accounting requirements.

When we have no ongoing legitimate business need to process your personal information, we will either delete or anonymize it or, if this is not possible (for example, because your personal information has been stored in backup archives), then we will securely store your personal information and isolate it from any further processing until deletion is possible.

8. Your Choices

We offer you choices regarding the collection, use, and sharing of your information.

Access and update your information

You can access and update certain information about yourself. For example, in the Leader Readiness Platform you can access your profile information by logging into your account. You can update your contact information, time zone, notification preferences, and photo within your profile. If you are an assessor, you can also update your availability in the assessor calendar. If you subscribe to our newsletter, you can update your profile by clicking Update Profile in the newsletter.

Delete your information

You may request deletion of your information by us, but please note that we may be required (by law or otherwise) to keep this information and not delete it (or to keep this information for a certain time, in which case we will comply with your deletion request only after we have fulfilled such requirements). When we delete any information, it will be deleted from the active database, but may remain in our archives.

Opt out of marketing communications

You may opt out of receiving promotional communications from us by using the unsubscribe link within each email or by contacting us as provided below to have your contact information removed from our promotional email list.

9. Our Policy about children

We do not intentionally gather information about visitors who are under the age of 18. If you are under the age of 18 you should not use our site or service.

10. Updates to this Privacy Policy

We may update this Privacy Policy because of changes of legal, technical or business developments. If we make any substantial changes in the way we use your information, we will notify you by sending you an e-mail to the last e-mail address you provided to us and/or by prominently posting notice of the changes on our website.

11. Privacy Shield

We continue to comply with the US-EU Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use, and retention of personal information from individual customers in the European Union member countries. Our participation in the Privacy Shield applies to all personal data that is subject to this policy and is received from the European Union and the European Economic Area. We are responsible for the processing of such personal data under the Privacy Shield Framework and subsequent transfers to a third party acting as an agent on its behalf. In particular, we remain responsible and liable under the Privacy Shield Principles if third-party agents that it engages to process the personal data on its behalf do so in a manner inconsistent with the Principles, unless we can prove that we are not responsible for the event giving rise to the damage. We certify that we adhere to the Privacy Shield Principles of notice, choice, and accountability for onward transfer, security, data integrity and purpose limitation, access, recourse, enforcement and liability. If there is any conflict between the policies in this privacy policy and 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 https://www.privacyshield.gov. The Federal Trade Commission (FTC) has jurisdiction over Company's compliance with the Privacy Shield. In compliance with the US-EU Privacy Shield Principles, Pinsight commits to resolve complaints about your privacy and our collection or use of your personal information. As further explained in the Privacy Shield Principles, a binding arbitration option will also be made available to you in order to address residual complaints not resolved by any other means.

12. How to contact us

We welcome your comments or questions regarding this Privacy Policy. Please e-mail us at dpo@pinsight.com or contact us at the following address or phone number: Pinsight, LLC, PO Box 18576, Denver, CO 80218, (800) 423-8295.