



Prometric Privacy Policy

Prometric is committed to protecting the personal data and information of employees, test candidates, website visitors and other individuals with whom we interact. We have a Global Privacy Policy that sets forth a formal process to protect the security and appropriate use of the Personal Data we collect for our own purposes and on behalf of our clients, the test sponsors. This Privacy Policy helps ensure that Personal Data is collected, transferred, and stored properly and in compliance with Data Protection Laws.

This Privacy Policy explains how we use, maintain and disclose personal data and information that we collect from individuals both online and offline, such as in our new hire processes, candidate registration and scheduling and test centers.

Table of Contents

- I. Privacy Notice**
- II. Information Security**
- III. Prometric’s Practices for the Collection and Use of Personal Data**
 - A. Personal Data**
 - B. How Prometric Collects Personal Data**
 - C. Privacy Statement for Biometrics (for Candidates)**
 - D. Individual Rights**
 - E. How Prometric Uses Personal Data**
 - F. Why Personal Data is Disclosed by Prometric**
 - G. Onward Transfer**
 - H. Notices to Residents of Countries Outside the United States**
 - I. Opt-Out Choices**
 - J. Access and Correction**
 - K. Privacy Policies of Third Parties**
 - L. Cookies and Other Data Collection Technologies**
 - M. Social Media Interactions**
 - N. Tell-a-Friend Functions**
 - O. Mobile Applications**
 - P. EU-U.S. Privacy Shield Certification**
 - Q. Swiss-U.S. Privacy Shield Certification**
 - R. U.S. Social Security Number Policy Statement**
 - S. California Privacy Rights**
- IV. Dispute Resolution Process**
- V. How to Contact Us**
- VI. Changes to Privacy Policy**

I. Privacy Notice

Prometric is committed to protecting the privacy and security of all personal data and information that we process in order to provide testing services to our clients, the test sponsors. This Privacy Notice provides a summary of our practices with regard to all of the personal data and information we collect and use in connection with testing services we offer for our clients, and includes personal data and information processed for the purpose of employing individuals to support those testing services.

Prometric collects and processes personal data and information only for legitimate business purposes. Personal data and information of exam candidates is collected and processed only as instructed or permitted by our clients, the test sponsors. We will collect and process that information that is reasonably needed to register an exam candidate for a test (including verifying eligibility to take an exam and verifying the identity of the exam taker), administer the exam (including protecting the security and integrity of the testing process), processing the exam results, and resolving any issues that may have occurred during the testing process.

If permitted under applicable law, we may communicate with exam candidates regarding other testing events offered by Prometric and our test sponsors. Candidates may opt-out of receiving these communications at any time, as provided below.

We may disclose candidate personal data and information to the applicable test sponsor, who will use that information in accordance with its own privacy policies.

Personal data and information of potential and/or active employees is collected and processed only for legitimate business purposes, including but not limited to, verifying identity and credentials, where allowed by law to process background checks and confirm suitability for employment, processing payroll, complying with statutory and regulatory employment requirements, and to confirm the safety and security of employees both on an on-going basis and in the event of a major weather or security-related event.

We will at all times maintain reasonable and appropriate security controls to protect the personal data and information of our candidates and employees. We have special controls to protect any sensitive personal data and information (such as government issued identification numbers and biometrics) that may be collected for security and identity verification purposes. For additional information about Prometric's information security practices please see below.

We may disclose personal data and information to our affiliates and data processors as needed to provide the services that candidates and the test sponsors have requested and to perform the functions necessary to run a global business. These entities are all contractually bound to limit use of all personal data and information they come in contact with as needed to perform only the services requested.

We will also always disclose personal data and information when required to do so by law, such as in response to a subpoena, to law enforcement agencies and courts with proper jurisdiction to request such information, or in response to regulatory inquiries.

Prometric will comply with the privacy and data collection and processing laws of the local jurisdiction of the individual from whom information is being collected. With the exception of biometric data, the personal data and information of exam candidates and employees based outside of the United States will be transferred, with the express consent of the individual, to Prometric, test sponsors and data processors in the United States and elsewhere in the world only to facilitate the purpose for which it was collected. Prometric will always protect the privacy and security of all personal data and information that it collects, regardless of where it is processed. Exam candidates located outside of the United States who do not provide the appropriate consent necessary for Prometric to transfer personal data and information to the

United States for processing understand that they may not be able to test with Prometric, and may be referred directly to their test sponsor for alternative testing solutions where available. Potential and active Prometric employees located outside of the United States who do not provide the appropriate consent necessary for Prometric to transfer personal data and information to the United States for processing of payroll and other employment related functions understand that they may not be eligible for employment with Prometric.

If you have questions about your privacy rights or other information related to Privacy, please see [Section V. "How to Contact Us"](#), below.

II. Information Security

Security protection is an undercurrent that runs through every part of Prometric's business. All of our technologies feature multiple layers of encryption and protection so constituents and stakeholders alike can rest assured that their intellectual property and Personal Data are being properly protected from theft while it is on our systems. We operate information technology facilities that meet or exceed industry standards, with secure back-ups at off-site locations, where all sensitive data is securely stored and protected.

Prometric draws on industry best practices and guidance from sources such as the National Institute of Standards and Technology (NIST), Payment Card Industry (PCI) and standards promulgated by the International Standards Organization (ISO) including, but not limited to, ISO/IEC 27018:2014 (Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors) and ISO/IEC 27001:2013 (Security techniques -- Information security management systems -- Requirements) to design and maintain its information security program. Prometric's Information Security Program is reviewed several times each year by multiple third party organizations to ensure it meets or exceeds the highest benchmarks available for security and data privacy.

III. Prometric's Practices for the Collection and Use of Personal Data

The following explains our practices with regards to all "Personal Data" collected and used by Prometric.

A. Personal Data

"Personal Data" is any non-public personal information, as such term is defined under Title V of the U.S. Gramm-Leach-Bliley Act, 15 U.S.C. s. 6801 et seq. and the rules and regulations issued thereunder; any "personal data" as defined in EU Directive 95/46/EC or any equivalent or similar concept of personal data or personal information under any applicable law; any "personal data" as defined in Malaysian Act 709 of the Personal Data Protection Act of 2010, or any other information that specifically identifies an individual, such as name, residential and office address or social security number, together, in each case, with any other information that relates to an individual who has been so identified and can be used to identify, locate or contact such individual. It includes, but is not limited to:

- Personal contact details
- Assessment details, including candidate ID number, examinations taken and when, scores related to those exams, how many times an exam or any particular section of exams have been taken;
- Employment information such as social security number, passport number or any other identifying information required by a government entity to confirm eligibility for employment;
- Credit card information;
- Residence and country of citizenship;

- Photographs;
- Signature;
- Audio and Video recordings;
- Fingerprint images and templates for Biometric Enabled Check-In;
- Information from identification, verification, or eligibility documents;
- Transaction and Relationship Information including elements that reveal candidate test patterns, test locations, test results, and information about how Prometric websites and applications are used.

B. How Prometric Collects Personal Data

In most cases, Prometric collects Personal Data directly from the individual through direct interactions including applying for employment and during the hiring process, registering on our website, scheduling a test or taking a test. In some cases, Prometric collects Personal Data from third parties. For example, we may receive information from employment agencies, test sponsors, or even from third party data suppliers who enhance our files and help us better understand our customers. These third parties may use cookies, web beacons, and other similar technologies to collect or receive information from Prometric’s website and elsewhere on the internet to provide us with data measurement services and target ads that address the search criteria of our customers.

When a candidate visits Prometric’s website, registers or takes an exam, uses our applications, or contacts us, we also collect transaction information for customer service purposes.

If an individual interacts with Prometric online, we use cookies and other technological tools to collect information about the use of our website and applications. We treat this information as Personal Data when it is associated with an individual’s Contact Information. For more information about cookies and other technologies, please see [Section M. Cookies and Other Data Collection Technologies](#), below.

To help ensure the security and integrity of the testing process, we may also collect information in our test centers using technological means, such as identification document scanners, fingerprint scanners, digital cameras, and audio-video surveillance monitoring equipment. In each case, we only use these technologies as permitted by applicable laws. If a candidate testing program uses a biometric enabled check in process at the test center, please see [Section C. Privacy Statement for Biometrics](#), directly below.

C. Privacy Statement for Biometrics (for Candidates)

Where selected by the test sponsor, Prometric’s Biometric Enabled Check-In System is designed to improve the security and integrity of the testing process in a way that protects test candidate privacy while ensuring test candidate identity. The Biometric Enabled Check-In System converts a fingerprint image to a digital image that is used for identity verification purposes, detects and prevents fraud and misrepresentation, maintains the integrity of the testing process, and improves the security of test centers.

1. How the Biometric Enabled Check-In System Works

By placing the index finger on a scanner in a Prometric Test Center, the Biometric Enabled Check-In System equipment captures an image of the fingerprint and creates a digitized representation of the fingerprint (a

"template"). The fingerprint image and template are paired with other Personal Data provided to Prometric by the candidate (such as name and other identifying information), allowing Prometric to identify the candidate accurately during the testing process and over repeated testing sessions for the same test sponsor.

For security purposes, all biometric data is securely transferred to and stored within Prometric's Central Data Center. Prometric manages the security and confidentiality of the data, to protect it from unauthorized access, use, disclosure, or alteration, and to retain and destroy the data in accordance with applicable law.

2. Purposes and Uses for Biometric Data

Biometric data is solely used by Prometric to: (1) administer tests and verify a candidate's identity on an ongoing basis as they participate in present and future assessments with the same test sponsor; (2) pre-populate candidate credentials at most Prometric test center facilities consequently reducing the time required during the check-in process; (3) detect and prevent fraud and misrepresentation by unauthorized candidates; (4) maintain the integrity of the testing process; (5) improve security of test centers by detecting and preventing unauthorized access to secure areas; and (6) as required by law.

3. Disclosures of Biometric Data

As a matter of policy, Prometric does not disclose biometric data to any third party (including test sponsors). However, in the event of an investigation of cheating, unauthorized testing, or other misconduct, Prometric may disclose the biometric data to the test sponsor or to law enforcement agencies and/or other third parties involved in the investigation of misconduct. Prometric will also disclose Personal Data, information and other records only in relation to lawful requests by regulatory, legal or government agencies with jurisdiction and/or authority to make such requests.

4. Security and Data Retention

Prometric and its subcontractors shall at all times protect a candidate's Personal Data with operational, administrative, technical and physical security safeguards. Unless a candidate's personal data or fingerprint images are being used in connection with an active security investigation; the test sponsor, Prometric and/or the biometric vendor on behalf of the test sponsor, shall retain candidate data collected through the Biometric Check-In System in accordance with the law in the jurisdiction in which the data was obtained, or for a maximum of five years from the date of the last assessment or the expiration of the purpose for which the candidate's data was collected; whichever time period is shorter, or as otherwise required by a test sponsor.

Other Personal Data collected by Prometric during test registration, new hiring, or any other administrative process is retained by Prometric in accordance with its record retention guidelines, and may also be sent to a test sponsors and/or retained in accordance with the test sponsor's record retention guidelines.

5. Data Processing

Prometric complies with all local privacy laws in the collection and processing of Personal Data or information, including biometric data such as fingerprint images. This includes but is not limited to, as required, providing disclosures on Prometric processes and procedures for the collection and processing of Personal Data (for example, this Privacy Policy and the Statements contained herein), obtaining consent of the individual, and/or adherence to local Data Protection Laws in the regions where Prometric conducts business. When a candidate submits to biometrics at a Prometric testing site, regardless of where the site is located globally, the biometric data is collected, transferred, processed and stored in Prometric's data center located in Ireland, where allowed by the applicable jurisdiction where the biometric data is collected.

Where required by law, candidates will be required to expressly consent to the collection, transfer and processing of Personal Data, including biometric data.

D. Individual Rights

A candidate or employee may, at any time:

- request access to and correction of Personal Data;
- make any inquiries, requests or complaints in relation to the use of Personal Data;
- withdraw consent to the processing of personal data (including fingerprint data)

In each case, the individual should direct requests and inquiries to Prometric's Data Protection Manager using the contact information in [Section V](#), "How to Contact Us" below. Complaints should be filed pursuant to the Dispute Resolution Process outlined in [Section IV](#).

E. How Prometric Uses Personal Data

Prometric uses Personal Data to fulfill requests for information and services, to administer testing programs securely and efficiently, and to operate our business. For example:

1. Test Candidates

- Prometric will respond to candidate requests for information about tests and testing opportunities, facilitate registration for exams, and provide testing services to both candidates and test sponsors (including test scheduling and administration, security and detection of cheating, test scoring, reporting and analysis of results, and customer service). Where permitted by law, Prometric may send exam candidates commercial communications and offers for additional testing or training services on behalf of test sponsors.
- Prometric, on behalf of its test sponsors, will use biometric data solely to: (1) administer the tests and verify identity, (2) protect privacy, (3) detect and prevent fraud and misrepresentation by unauthorized candidates, (4) maintain the integrity of the testing process, (5) preserve security of test centers by detecting and preventing unauthorized access to secure areas, and (6) as required by law.

2. Employees (Potential, Active & Former)

- Prometric will use information supplied by individuals who have applied for employment with Prometric for recruitment and other customary human resources purposes, such as payroll processing, business continuity and disaster recovery planning, and to satisfy corporate governance and regulatory obligations.

Prometric will also use Personal Data collected from employees to document employment-related decisions and to comply with government record keeping and reporting requirements. By law, Prometric must maintain certain personnel records on applicants and current and past employees. The Human Resources department is responsible for overseeing the record keeping for all personnel information. Access to information is limited to persons inside Prometric who need to know for business purposes and released to persons outside of Prometric only with authorization or as required by law. Employees may view their personnel file by submitting a request to Human Resources. Upon receipt of this request, an appointment will be scheduled during which the employee may view their file in the presence of a member of the Human Resources Department.

3. Legitimate Business Purposes

- Prometric also uses Personal Data as needed to manage everyday business needs such as payment processing and financial account management, backup purposes to facilitate business continuity, test center management, business planning, contract management, website administration, fulfillment, analytics, security and fraud prevention, corporate governance, business continuity and disaster recovery planning, auditing, reporting and compliance with any legal or regulatory obligations.

F. Why Personal Data Is Disclosed by Prometric

Prometric **DOES NOT** share Personal Data with third parties for their own marketing purposes. Prometric requires its subcontractors and vendors who have access to Personal Data to provide, at a minimum, the same levels of protection as provided by Prometric concerning Personal Data. Where Prometric is required to transfer Personal Data onward to a third party to further the performance of a legitimate business purpose, Prometric will remain liable for the proper use, processing, and storage of such data in a manner that is consistent with the purposes for which it was collected. We limit our sharing of all Personal Data as follows:

1. Test Candidates

- Prometric may disclose Personal Data of exam candidates to test sponsors, which will use and disclose Personal Data in accordance with their own privacy policies. Prometric acts as a processor for test sponsors, who are our clients. We send candidate Personal Data and test results to the test sponsors so that they can provide candidates with the accreditation, service, license or credentials sought.
- Prometric may share Personal Data with our affiliates and authorized test centers, which may only use Personal Data for the purposes listed above. For example, we will provide Personal Data to the test center so that it is prepared for exam candidates on test day.
- Prometric may share Personal Data with our service providers to facilitate candidate and test sponsor requests. Service providers are bound by law or contract to protect Personal Data and only use such Personal Data in accordance with Prometric's requirements and instructions.

2. Employees (Potential, Active & Former)

- Prometric may share Personal Data with our service providers, such as our payroll processors, benefits providers, and performance measurement vendors to facilitate employee compensation, benefit elections and claims, and performance and growth goals, objectives and milestones. Service providers are bound by law or contract to protect Personal Data and only use such Personal Data in accordance with Prometric's requirements and instructions.

3. Legitimate Business Purposes

- Prometric may disclose Personal Data where needed to affect the sale or transfer of business assets, to enable payment processing, to enforce our rights, protect our property, or protect the rights, property or safety of others, or as needed to support external auditing, compliance and corporate governance functions. We will also disclose Personal Data when required to do so by law, such as in response to a subpoena including to law enforcement agencies and courts in the United States, Member-States of the European Union, India, Malaysia, China, Japan and other countries where we operate.

4. Investigative, Legal & Government Requests

- In the event of an investigation of cheating, unauthorized testing, or other misconduct, Prometric may disclose the biometric data to the test sponsor or to law enforcement agencies and/or other third parties involved in the investigation of misconduct. We also may provide access to Personal Data when legally required to do so, to cooperate with police investigations or other legal proceedings, to protect against misuse or unauthorized use of our intellectual property, to limit our legal liability and protect our rights, or to protect the rights and safety of our employees, candidates, clients or the public. In those instances, the information is provided only for that limited purpose.

Please note that we may also use and disclose information about an individual that is not considered Personal Data. For example, we may publish reports that contain aggregated and statistical data about our test candidates or website visitors. These reports do not contain any information that would enable the recipient to contact, locate or identify the individual that is the subject of the information disclosed.

We will not share Personal Data in ways unrelated to those described above without providing an individual with an opportunity to opt out of such use or disclosure or otherwise prohibit such unrelated uses or disclosures.

G. Onward Transfer

Prometric may employ other companies and individuals to perform functions on our behalf which require us to transfer Personal Data and other information to a third party data controller, processor or vendor. Our employees, agents and contractors who have access to Personal Data and information are contractually required to protect the information in a manner that is consistent with this Privacy Policy and the principles of the Privacy Shield with regards to transfer, processing or use of Personal Data. We do not transfer information to third parties who are not acting in a contractual capacity as Prometric's agent or on Prometric's behalf. Prometric will, at all times, remain liable for Personal Data that it transfers onward to a third party.

H. Notices to Residents of Countries Outside the United States

Prometric is headquartered in the United States of America. All Personal Data of International candidates, with the exception of biometric data, who do business with or international employees who are employed by Prometric will be accessed from or transferred to the United States, or to our affiliates and data processors elsewhere in the world for the appropriate processing, use and storage. "International candidates" and "international employees" are candidates or employees residing outside of the United States on a permanent basis who do not hold a United States passport. All international candidates and employees will be required to provide express consent for the collection, transfer and processing of Personal Data to the United States. By continuing to provide Prometric with Personal Data, through registration or scheduling as an exam candidate or through the employment hiring process, a candidate or employee continues to consent to the transfer of Personal Data to the United States until such consent is expressly withdrawn in writing to Prometric's Data Protection Manager using the contact information provided below. Prometric will always protect the privacy and security of Personal Data pursuant to our Information Security Guidelines, Policies and Procedures, regardless of the location where it is originally collected or ultimately processed or stored.

I. Opt-Out Choices

Individuals can always limit the information provided to Prometric. However, Prometric abides by the policies of its clients, the test sponsors, regarding the Personal Data of candidates that must be collected

in order for Prometric to administer a test on behalf of the test sponsor. Individuals that do not wish to provide Personal Data required by the test sponsor will need to contact the test sponsor to make other testing arrangements.

As permitted by applicable law, individuals may also withdraw consent to the processing of Personal Data. However, exercising this right may prevent Prometric's ability to deliver any further assessments from the test sponsor to the individual withdrawing consent, and the test sponsor may refuse to distribute the individual's exam results.

Commercial Emails/Direct Marketing

Individuals can limit the communications that Prometric sends via direct marketing. To opt-out of commercial emails, simply click the link labeled "unsubscribe" at the bottom of any email sent by Prometric. Please note that even if opting-out of commercial emails, Prometric may still need to contact candidates with important transactional information about their Prometric account or scheduled exam. For example, Prometric will still send testing confirmations and reminders, information about test center changes and closures, and information about test results even if commercial emails have been opted-out.

Third-Party Ad Targeting

To opt out of being targeted by many third party advertising companies, third parties that collect or receive information from mobile applications and use that information to provide measurement services and targeted advertising, or for more information about third party advertising please visit the Network Advertising Initiative (NAI) at www.networkadvertising.org. Individuals may also visit www.aboutads.info/choices to learn about opting-out of third-party collection and use of information for ad targeting. Prometric will never provide Personal Data to third parties other than for the purpose for which the Personal Data was originally collected.

For questions about opt-out choices or for assistance with opting-out, please contact Prometric's Data Protection Manager using the contact information in Section V. "How to Contact Us", below. If sending a letter, please include name, address, email address, and a brief explanation of the opt-out communications request.

J. Access to Personal Data

1. Access & Correction

Prometric respects an individual's right to access and correct their Personal Data. Exam candidates and Prometric employees have the right with respect to access to:

- obtain confirmation from Prometric of whether or not Personal Data that relates to them is being processed;
- have such data communicated to them so that verification of its accuracy and lawfulness of the processing can be confirmed; and
- have the data corrected, amended or deleted where it is inaccurate or processed in violation of applicable law.

Exam candidates and Prometric employees may request access to and correction of their Personal Data at any time; however, must supply Prometric with sufficient information to allow us to confirm the identity of the person making the request for access. Candidates and employees may even self-correct such information by performing the following:

For candidates with an online account, simply log into the account at any time to access and update the information provided to Prometric.

Employees may update their Personal Data by logging into Dayforce and updating their profile information.

For assistance updating Personal Data, please contact Prometric using the contact information in Section V. "How to Contact Us", below.

2. Restriction to Access

Prometric will only restrict access to information to the extent that disclosure is likely to interfere with the safeguarding of important countervailing public interests, or to the extent that the requests for access become so excessive and/or repetitive as to cause an undue burden to the organizational resources that must be expended in order to fulfill such requests. In such a situation, Prometric may charge a fee for excessively repetitive requests for access to cover the costs of its resources to fulfill such requests. In addition, where personal information is processed solely for research or statistical purposes, access may be denied. Other reasons that Prometric may deny or limit access include:

- Interference with the execution or enforcement of the law or with private causes of action, including the prevention, investigation or detection of offenses or the right to a fair trial;
- Disclosure where the legitimate rights or important interests of others would be violated;
- Breaching a legal or other professional privilege or obligation;
- Prejudicing employee security investigations or grievance proceedings or in connection with employee succession planning and corporate re-organizations; or
- Prejudicing the confidentiality necessary in monitoring, inspection or regulatory functions connected with sound management, or in future or ongoing negotiations involving the organization.

K. Privacy Policies of Third Parties

This Privacy Policy only addresses the use and disclosure of information by Prometric. Test sponsors have their own privacy policies and data collection, use and disclosure practices, and Prometric is not responsible for compliance with their practices. All individuals are encouraged to familiarize themselves with the privacy policies and data collection practices of any organization that they interface with.

L. Cookies and Other Data Collection Technologies

When an individual visits the Prometric website or uses Prometric's mobile applications, we collect certain information by automated means, using technologies such as cookies, pixel tags, browser analysis tools, server logs, web beacons, and other similar technologies to ensure that the Prometric website offers the best possible experience. In many cases, the information we collect using cookies and other tools is only used in a non-identifiable way, without any collection of Personal Data. For example, we use information we collect about all website users to optimize Prometric websites and capabilities, to understand and measure website traffic patterns, and to send target offerings based on such patterns. **Use of the Prometric website indicates a user's agreement to the use of cookies and consent to receive other cookies that may be presented while visiting the Prometric website.**

In some cases, Prometric does associate the information collected using cookies and other technology with an individual's Personal Data.

1. Types of data collected and technologies used:

- When an individual visits the Prometric website, cookies may be placed on the individual's technological device. Cookies are small text files that websites send to a computer or other Internet-connected device to uniquely identify a browser or to store information or settings in a browser. Cookies allow a website provider to recognize a repeat user of the website each time the user returns. Cookies also help a website provider deliver a customized experience to each user and enable a website provider to detect

certain kinds of fraud. In many cases, individuals can manage cookie preferences and opt-out of having cookies and other data collection technologies used by adjusting the settings on their browsers. All browsers are different, but visiting the "help" section of a browser to learn about cookie preferences and other privacy settings may be of assistance.

- Prometric websites may use Flash Cookies (also known as Local Stored Objects) and similar technologies to personalize and enhance each individual's online experience. The Adobe Flash Player is an application that allows rapid development of dynamic content, such as video clips and animation. Prometric uses Flash cookies for security purposes and to help remember settings and preferences similar to browser cookies, but these are managed through a different interface than the one provided by an individual's web browser. To manage Flash cookies, please see Adobe's website at <http://kb2.adobe.com/cps/526/52697ee8.html> or visit www.adobe.com. Prometric does not use Flash cookies or similar technologies to serve its own interest-based advertising.
- Pixel tags and web beacons are tiny graphic images placed on website pages or in some Prometric emails that allow us to determine whether an individual has performed a specific action. When an individual accesses these pages or opens or clicks on an email the pixel tags and web beacons generate a notice of that action. These tools allow Prometric to measure responses to our communications and improve our web pages and promotions.
- Prometric server logs and other tools collect information from devices used to access Prometric websites, such as operating system type, browser type, domain, and other system settings, as well as the language a system uses and the country and time zone where the device accessing the Prometric website is located. Prometric server logs also record the IP address of the devices used to connect to the Internet, and may enable Prometric to collect information about the websites being visited by an individual before and after accessing the Prometric site. Collecting IP addresses and related data is standard practice on the Internet, and Prometric treats IP addresses as Personal Data. We use IP addresses for purposes such as calculating website usage levels, helping diagnose server problems, administering the website and combating fraudulent and/or malicious web activity. We also collect customary information from web browsers, such as Media Access Control (MAC) addresses, device type, screen resolution, operating system version and internet browser type and version. Prometric uses this information to ensure that our websites function properly for all devices and browsers and for security purposes.

Prometric may have relationships with third party advertising companies to place advertisements on its websites and to perform analytics and reporting functions for its websites. These third party advertising companies may place cookies on individual's computers when visiting Prometric's website so that the website can display targeted advertisements to the user. Prometric expects third party advertising companies to use reasonable efforts to respect browser do-not-track signals by not delivering targeted advertisements to website visitors whose browsers have a do-not-track setting enabled. Additionally, Prometric does not knowingly allow these third party advertising companies to collect Personal Data in this process, and does not give any Personal Data to them.

To learn about how to opt-out of third party collection and use of information for ad targeting please see [Section J. - Opt-Out Choices, Third Party Ad Targeting](#).

M. Social Media Interactions

Prometric's websites offer each individual user the ability to share content with friends using social media, such as Facebook and Twitter. Use of the "like" button, sharing buttons and other tools are subject to each social media platform's privacy policies.

Prometric websites also use Facebook Social Plugins. If a user is logged into Facebook while browsing on Prometric's website, Facebook Social Plugins allows Facebook to share information about a user's activities on Prometric's website with other Facebook users who use Prometric's website. For example, Social Plugins allows Facebook to show a user's Likes and comments on Prometric pages to the user's Facebook friends. Facebook Social Plugins also allows users to see their friends' Facebook activity on Prometric's website. Prometric does not receive or control any of the content from Facebook Social Plugins. For more information about Facebook Social Plugins and other social media tools, [click here](#).

Prometric may allow a website user to sign in to their online account using Facebook Connect. If an individual chooses to do this, we may collect information necessary to facilitate social interactions such as friend lists, birthday, check-ins, basic profile information and the user's profile picture, but only if the privacy settings selected by the individual within Facebook allow it. Prometric will use the information collected to create and facilitate an interactive social experience. In doing so, we will always comply both with the terms of this Privacy Policy as well as with Facebook Connect terms regarding use of Facebook profile information.

N. Tell-A-Friend Functions

Prometric offers "tell-a-friend" functionality on our websites. If individuals choose to use this function, we will collect Contact Information of a user's friends. We will automatically send the friends a one-time email with the information specified or inviting them to visit the Prometric site. Prometric uses this information for the sole purpose of sending a one-time email and does not retain the information.

O. Mobile Applications

Prometric offers mobile applications that allow individuals to access their Prometric accounts, interact with Prometric online and receive other information via smartphones and devices. All Personal Data collected by Prometric via our mobile applications is protected and processed only by the terms of this Privacy Policy.

When an individual downloads Prometric's mobile applications, he or she may choose to allow Prometric to obtain their precise location from the mobile device. We use this information to customize our response to candidate and potential customer requests. For example, if a candidate is searching for a test center we can display only ones in their area based on the location of the mobile device and provide access to real-time maps. We may also offer automatic ("push") notifications. Prometric will provide push notifications only to those customers who opt-in to receive such notifications from us. No one is required to provide location information to Prometric or to enable push notifications to use any of our mobile apps. Questions about location and notification privacy should be directed to mobile service providers or the manufacturer of such devices to learn how to adjust location and privacy settings.

To learn about how to opt-out of third party collection and use of information for ad targeting please see [Section J](#). - Opt-Out Choices, Third Party Ad Targeting.

P. EU-U.S. Privacy Shield Certification

Prometric maintains self-certification for and complies with the EU-U.S. Privacy Shield Principles regarding the collection, use, and retention of Personal Data from individuals located in the European Economic Area and other countries that recognize the principles of the Privacy Shield Framework for the collection, transfer and processing of Personal Data to the United States. Prometric commits to the Privacy Shield Principles including, but not limited to notice, choice, onward transfer, security, data integrity and purpose limitation, access, and recourse, enforcement, and liability for all Personal Data received from individuals residing in the EU. Prometric submits to the investigatory and enforcement powers of the United States Federal Trade

Commission ("FTC") related to all matters concerning Personal Data and privacy. To learn more about the Privacy Shield program, and to view Prometric's certification, please visit <https://www.privacyshield.gov/>.

Q. Swiss-U.S. Privacy Shield Certification

Prometric maintains self-certification for and complies with the Swiss-U.S. Privacy Shield Principles regarding the collection, use, and retention of Personal Data from individuals located in Switzerland for the collection, transfer and processing of Personal Data to the United States. Prometric commits to the Privacy Shield Principles including, but not limited to notice, choice, onward transfer, security, data integrity and purpose limitation, access, and recourse, enforcement, and liability for all Personal Data received from individuals residing in Switzerland. Prometric submits to the investigatory authority and enforcement powers of the United States Federal Trade Commission ("FTC") and, where applicable, to the Swiss Data Protection and Information Commissioner related to all matters concerning Personal Data and privacy. To learn more about the Privacy Shield program, and to view Prometric's certification, please visit <https://www.privacyshield.gov/>.

R. U.S. Social Security Number Protection Policy Statement

Prometric collects Social Security numbers and other sensitive Personal Data in the ordinary course of business related to employees, and only where required by the test sponsor for candidates. We have implemented reasonable technical, physical and administrative safeguards to help protect the Social Security numbers and other sensitive Personal Data from unlawful use and unauthorized disclosure. Prometric associates and contractors are required to follow these established procedures, both online and offline.

Access to Social Security numbers is limited to those employees and contractors who have a need to access the information to perform contractual obligations for Prometric. Social Security numbers are only disclosed to third parties in accordance with Prometric's established policies in accordance with a legitimate business purpose. Prometric will only disclose Social Security numbers to those test sponsors, service providers, auditors, advisors, and/or successors-in-interest who are legally or contractually obligated to protect them or as required or permitted by law.

S. California Privacy Rights

California Civil Code Section 1798 allows California residents to ask companies with whom they have an established business relationship to provide certain information about the companies' sharing of Personal Data with third parties for direct marketing purposes.

Prometric does not share any California consumer Personal Data with third parties for marketing purposes without consent.

If you are a test candidate, Prometric will provide your Personal Data to your test sponsor, who may use the information in accordance with its own privacy policies.

California residents who wish to request further information about Prometric's compliance with this law or have questions or concerns about Prometric's privacy practices may contact us using the contact information in [Section V](#), "How to Contact Us", below.

IV. Dispute Resolution Process

A. Filing Complaints

Exam candidates and employees who have concerns or complaints regarding Prometric's collection and processing of Personal Data must first utilize Prometric's internal complaint resolution process by contacting Prometric's Data Protection Manager using the contact information in Section V, "How to Contact Us", and providing a detailed written description of the issue and/or complaint. Prometric will respond to all complaints related to Personal Data issues in forty-five (45) days or less.

B. Independent Recourse Mechanism

1. Candidates

After exhausting Prometric's internal complaint process, if an exam candidate is not satisfied with the resolution, he or she may file a complaint with the Better Business Bureau Council of Greater Maryland ("BBB"), an alternative dispute resolution provider based in the United States. Prometric is an A+ accredited business with the BBB, and the BBB will review all complaints and make a determination as to whether the complaint should be referred for arbitration or mediation.

BBB Website: <http://www.bbb.org/greater-maryland/>

BBB Telephone: 410-347-3990

BBB Fax: 410-347-3936

2. Employees

Employees that have exhausted the internal mechanism for filing complaints above, or who are uncomfortable utilizing such mechanism, should submit complaints, concerns or inquiries to Prometric's Ethics Committee for review. Information on submission of complaints or inquiries to the Ethics Committee can be found in the Prometric Code of Business Conduct, *Confidential and Anonymous Reporting*.

C. Additional Recourse Mechanisms under Privacy Shield

With respect to Personal Data of residents of the European Union and Switzerland under the EU-US/Swiss-US Privacy Shield Principles (both candidate and human resource/employee data), Prometric has further committed to refer unresolved privacy complaints and to cooperate with the EU DPAs under the EU-U.S. Privacy Shield and the Swiss Federal Data Protection and Information Commissioner FDPIC under the Swiss-U.S. Privacy Shield by providing recourse for individuals to whom the data relates, implementing follow-up procedures for verifying that the attestations and assertions made in this Privacy Policy are true, and taking responsibility for obligations to remedy problems arising out of any failure to comply with the Principles and the consequences thereof. Prometric will cooperate with the DPAs and/or FDPICs in any investigation or resolution of complaints brought under the Privacy Shield and will comply with any reasonable advice given by the DPAs or FDPICs where the DPAs or FDPICs take the view that Prometric needs to take specific action to comply with the Privacy Shield Principles.

If you do not receive timely acknowledgment of your complaint, or if your complaint is not satisfactorily addressed, please visit www.privacyshield.gov for more information and to file a complaint.

D. Arbitration

Prometric will submit to arbitration for certain residual claims only where claimed violations of the Privacy Shield Principles have not been resolved after exhausting all of the available dispute resolution mechanisms above. An individual who wishes to invoke arbitration must take the following steps prior to initiating an arbitration claim: (1) raise the claimed violation directly with Prometric and afford Prometric with an opportunity to resolve the issue within 45-days; (2) make use of the independent recourse mechanism; and (3) raise the issue through their local Data Protection Authority to the U.S. Department of Commerce ("USDOC") and afford the USDOC with an opportunity to resolve the issue.

This arbitration option may not be invoked if an individual's same claimed violation of the Privacy Shield Principles (1) has previously been subject to binding arbitration; (2) was the subject of a final judgment entered in a court action to which the individual was a party; (3) was previously settled by the parties; or (4) if an EU Data Protection Authority has authority to resolve the claimed violation directly with the organization.

V. How to Contact Us

Please contact Prometric directly with any questions or comments about our privacy practices or this Privacy Policy and the statements contained herein. You can reach us via email at DataProtectionManager@prometric.com or via mail to:

Data Protection Manager
Legal Department
Prometric Inc.
1501 South Clinton Street
Baltimore, Maryland 21224 USA

If sending a letter, please include name, address, email address, and a brief explanation of your information request, inquiry or complaint.

For inquiries or assistance related to time sensitive issues concerning exams such as scheduling, cancellations, eligibility, payment, name changes or other test related issues, please visit <https://www.prometric.com/en-us/contact-us/pages/default.aspx> for the most expeditious resolution of your issue.

VI. Changes to Privacy Policy

From time to time, Prometric may update this Privacy Policy to reflect new or different privacy practices or changes to the law. We will place a notice online when we make material changes to this Privacy Policy or the statements contained herein. Additionally, if the changes will materially affect the way we use or disclose previously-collected Personal Data, we will notify impacted individuals about the change by sending a notice to the primary email address associated with the account impacted.