"Information Security is a Responsibility that we all share!"

Privacy Policy

Maintenance: This document falls under documentation control and it is reviewed at least annually by responsible parties within Prometric and updated as necessary.
Notice: Printed versions of this document may not be current. Verify issue date against the online system.

PROMETRIC PRIVACY POLICY

OUR COMMITMENT

Prometric is committed to protecting the personal data and information of employees, test candidates, contractors, vendors, website visitors and other individuals with whom we employ or provide services to. We have a Global Privacy Program that sets forth a formal process to protect the security and appropriate use of the Personal Data we collect for our own legitimate business purposes and on behalf of our clients, the test sponsors.

This Privacy Policy helps ensure that Personal Data is processed properly and in compliance with all applicable data protection laws. It explains how we use, maintain and disclose personal data and information that we collect and/or have access to through the course of our business. This policy covers any current or former employee, test candidate, contractor or partner about whom this organization processes data.

Please contact Prometric directly with any questions or comments about our privacy practices or this Privacy Policy and the statements contained herein. To submit a request related to your personal data, please click on the following link Personal Data Requests and complete all of the fields required in the form.

Table of Contents

I. Information Security

A. Data Security & Confidentiality

Security of information, both personal and proprietary data, is an undercurrent that runs through every part of Prometric's business. All of our technologies feature multiple layers of encryption and protection so that our test candidates, clients, employees, constituents and stakeholders alike can rest assured that their personal data and intellectual property are being properly protected from theft, loss, improper copying, modification or tampering, improper retention or destruction, loss of integrity or unauthorized access, use or disclosure while it is in our systems. We operate information technology facilities that meet or exceed industry standards, with secure back-ups at off-site locations, where all personal data and intellectual property are 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 and protection.

Prometric takes all reasonable steps to ensure that appropriate security measures are in place to protect the confidentiality of both electronic and manual data. Any person handling personal data on behalf of Prometric is bound by a contract including, amongst other safeguards, a confidentiality obligation regarding personal data (e.g., in the third party services agreement, employment contracts, Prometric Code of Business Conduct and Ethics, etc.) obligations to take appropriate steps to prevent the misuse or loss of personal data and to prevent unauthorized access to it. In addition, third parties are under the obligation to immediately report any known or suspected instance of misuse, loss or unauthorized access to their manager, or Data Protection Officer.

Security measures will be reviewed from time to time, having regard to the technology available, the cost and the risk of unauthorized access. Employees must implement all organizational security policies and procedures, e.g. use of computer passwords, locking filing cabinets, encryption of data being sent electronically, etc.

Employees who have access to records and files that contain personal data must ensure that they treat them confidentially and must not disclose it, except in the course of their employment. All employees will have access to a certain amount of personal data relating to colleagues, customers or other third parties. Employees must play their part in ensuring its confidentiality. They must undergo Privacy and Data Protection training at the point of on-boarding and at least annually thereafter. Part of such training requires employees to adhere to the following data protection principles:

- Process data fairly, lawfully and transparently
- Keep data only for specified, explicit and legitimate purpose(s)
- Process data only in ways which are compatible with the purpose(s) for which it was given
- Keep personal data accurate and up-to-date throughout the information lifecycle (i.e., from collection to destruction)
- Respond promptly to: requests to access, cease collecting / processing, modify or remove personal data held by Prometric; requests to exercise a data subject's right of data portability.

• Ensure data is adequate, relevant and limited to what is necessary for the purpose for which it was given

• Keep data safely and securely

• Retain personal data for no longer than is necessary for the purpose for which it is processed and in line with the company's data retention policy

• Promptly report any Data Privacy Breach

Employees must not disclose personal data, except where necessary in the course of their employment, or in accordance with law. They must not remove or destroy personal data except for lawful reasons and with the permission of the organization. Any breach of the data protection principles or this Privacy Policy is a serious matter and may lead to disciplinary action up to and including dismissal. If employees are in any doubt regarding their obligations, they should contact their direct supervisor or Prometric's Privacy Program Manager.

B. Data Breach Management

A Personal Data Breach occurs when there is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise Processed. "Unauthorized" means that it occurs in contravention of applicable privacy legislation or applicable privacy policies.

Some of the most common privacy breaches happen when personal data of employees, consumers or customers is stolen, lost or mistakenly disclosed (e.g., a computer containing personal data is stolen or personal data is mistakenly emailed to the wrong recipient). A data breach may also be a consequence of faulty business procedure or operational break-down.

If a data breach is suspected as having occurred then it is imperative to immediately notify the Senior Manager of IT Security Leader or the Data Protection Officer.

II. Prometric Practices with Respect to Personal Data

The following explains our practices with regards to all "Personal Data" collected and processed by Prometric. For the purposes of this policy "data subjects" include employees, test candidates, or partners, independent contractors or vendors under a service contract with Prometric and for whom Prometric has access to personal data to facilitate a legitimate business purpose.

A. Collect and use Personal Data fairly and lawfully

A fundamental Data Privacy principle requires that Prometric collect and process personal data fairly and lawfully. When collecting and processing personal data, Prometric must consider relevant laws and regulations in addition to this Policy.

The following principles must be followed by those subject to the Policy:

- Collect and use personal data only with a legal justification which may include the legitimate business interests of Prometric. For example, guidelines or local laws may require explicit consent of the data subject prior to collecting personal data.

- Notify data subjects about how their personal data will be used prior to collecting their personal data. This notification includes explanations of how the data subject can exercise their rights, including the right to file a complaint with a supervisory authority.
- Collect only the personal data needed for a specific business purpose.
- Use personal data only for the specific business purpose described in the Privacy Notice or Consent form or in a way that the person would reasonably expect.
- Use personal data in ways that do not have an adverse effect on the person concerned unless such use is justified by law.
- Anonymize or Pseudonymize personal data when possible or appropriate, and make use of the principle of data minimization (only collect the minimum of personal data needed for the business purpose).

Compliance with the above principles can be ensured by completing a Privacy Impact Assessment (PIA) prior to the development and marketing of new brands, products or services.

B. 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 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016; any "personal data" as defined in Malaysian Act 709 of the Personal Data Protection Act of 2010, or any equivalent or similar concept of personal data or personal information under any applicable law, or any other information that specifically relates to or identifies an individual and can be used to identify, locate or contact such individual. It includes, but is not limited to:

- Personal contact details (name, address, telephone number, country-specific identification number, email address, login and password information)
- Date of birth, gender, race, ethnicity, and sexual orientation
- Health information or medical data
- Assessment details, including test 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, passport or Visa number or any other identifying information required by a government entity to confirm eligibility for employment;
- Credit card and financial institution information;
- Residence and country of citizenship;
- Photographs;
- Signature;
- Audio and Video recordings;
- Biometrics (fingerprint images and templates, facial images);

- 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.

Personal data such as race, ethnicity, sexual orientation, health information, or biometrics are sensitive data according to EU data protection requirements and as such shall be subject to enhanced security measures as applicable under EU law.

1. Purposes for Personal Data Collection & Processing

Personal data is collected solely to: (1) process applications for employment and onboarding during the hiring process, (2) register for or schedule a test, (3) take a test, or (4) in some cases, process Personal Data from third parties in furtherance of the examples outlined above. In most cases Prometric collects such Personal Data directly from the individual data subject. However, in some cases we may receive information from employment agencies, test sponsors, or even from third party data suppliers to enhance our files and help us better understand 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 information that has the effect of identifying an individual.

To help ensure the security and integrity of the testing process, we may also collect information in our corporate offices or test centers using technological means such as identification document scanners, fingerprint scanners, digital cameras, and audio-video surveillance monitoring equipment (see *Biometric Data,* below). In each case, we only use these technologies as selected and/or approved by a test sponsor and as permitted by applicable laws.

2. Disclosure of Personal Data

Prometric **DOES NOT** share Personal Data with third parties for their own marketing purposes. Prometric also does not transfer information to third parties who are not acting in a contractual capacity as Prometric's agent or on Prometric's behalf.

Employees who share personal data with third parties for other business-related purposes must obtain assurance that the third party has the ability and intention to protect personal data, consistent with the standards and principles contained in this Policy. This may be done through third party due diligence, risk assessments, and/or a formal written contract.

A processing agreement is required whenever a third party is provided access to personal data in order to process such personal data on behalf of the company. In addition, a similar agreement may be required when one Prometric affiliate processes personal data on behalf of another affiliate. These agreements may take the form of contracts between affiliates, or standard contracts with third parties. All agreements must include the Data Privacy principles and processing instructions.

Based on risk assessments conducted on third parties, appropriate technical safeguards (e.g., encryption) or other remedial measures need to be provided for by contract to ensure adequate protection of personal data.

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:

a. Test Candidates

- Prometric acts as a processor for test sponsors, who are our clients. Prometric may disclose Personal Data of test candidates to test sponsors who manage the data pursuant to their own privacy policies. We send candidate Personal Data and test results to the test sponsors so that they can provide candidates with the accreditation, service, license or credential sought.

- Prometric may share Personal Data with our affiliates and authorized test centers which may only use Personal Data for the purposes outlined herein. For example, we will provide Personal Data to the test center so that it is prepared for a test candidate's arrival on test day.

- Prometric may share Personal Data with our service providers (vendors) to facilitate candidate and test sponsor requests. Service providers are bound by law or contract to protect Personal Data and only process such data in accordance with contractual obligations and responsibilities.

b. Employees (Potential, Active & Former)

- Prometric may share Personal Data with our service providers (vendors), such as 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 contractual obligations and responsibilities.

c. Legitimate Business Purposes

- Prometric may disclose Personal Data where necessary in furtherance of 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.

d. Investigative, Legal & Government Requests

- Prometric may disclose Personal Data where necessary to facilitate an investigation of cheating, unauthorized testing, or other misconduct. We also may disclose or provide access to Personal Data when legally required to do so, such as in response to a subpoena or summons, to cooperate with law enforcement or other legal proceedings in the countries where we operate, or 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 each instance, the information that is provided is limited to the extent necessary and appropriate.

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.

3. Retention and Storage of Personal Data

Prometric promulgates a comprehensive Records Management Program and Schedule that it adheres to for the purposes of retention, storage and destruction of all records created in the course of its business including those containing personal data. We also deploy a Data Management strategy that segregates data, to the extent feasible, based on regionally located data servers in the United States, Ireland and Japan.

At all times Prometric protects personal data with operational, administrative, technical and physical security safeguards. Unless personal data is being used in connection with an active security investigation Prometric shall retain personal data for the lesser period of:

- five (5) years from the date of the last service, test or assessment; or
- the expiration of the purpose for which the personal data was collected; or
- the laws of the applicable jurisdiction where the data was collected.

Personal data shall only be retained for a greater period where (1) required by law or regulation for the purposes of recordkeeping requirements or (2) prescribed by contract and permissible under the laws of the applicable jurisdiction.

C. Biometric Data

Prometric collects biometric data of test candidates where the service is selected by a test sponsor, as well as from employees who are located in certain Prometric corporate offices.

The 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 confirming test candidate identity. The system is also utilized to facilitate access to controlled secure areas of Prometric's corporate administrative offices. 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, improves the security of test centers, and allows controlled access to restricted and secure areas of Prometric's corporate locations.

By placing an index finger on a scanner 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 individual data subject (such as name and other identifying information) allowing Prometric to confirm the individual's identify on an on-going basis.

1. Purposes for Biometric Data Collection & Processing

Prometric, on behalf of its test sponsors, will collect 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. Disclosure of Biometric Data

As a matter of policy, Prometric does not disclose biometric data to any third party except as outlined herein. Prometric may disclose biometric data to a test sponsor, law enforcement agency, or a third party

that is under contract with Prometric or compelled by applicable law to be involved in an investigation related to alleged misconduct solely for the purposes of an investigation of cheating, unauthorized testing, or other test candidate misconduct. Prometric may also disclose biometric data only in relation to lawful requests by regulatory, legal or government agencies with jurisdiction and/or authority to make such requests.

3. Retention and Storage of Biometric Data

All exam candidate biometric data is securely transferred to and stored within Prometric's Data Center located in Ireland. Biometric data of employees is retained in the respective security systems, most of which reside at the Prometric office where the data was collected. Biometric data is retained for 5-years from the last service, test, or assessment for exam candidates. Biometric data of employees is retained for 1-year from the date of termination of employment. In all cases biometric data if retained for shorter period as required by applicable law in the jurisdiction where the data was collected.

D. Medical Data

Occasionally, and only in specific Prometric office locations, it may be necessary to refer employees to an independent Occupational Physician for a medical opinion or second opinion in accordance with the local sick pay policy. Other examples of medical data that Prometric may have access to include doctor's certificates/notes after an employee has been out of work for an illness.

Prometric also receives, in very limited circumstances, medical data related to test candidates' requests for testing accommodations.

In each of these instances Prometric may receive certain medical information which will be stored in a secure manner with the utmost regard for the confidentiality of the information contained therein. Medical data is not retained for any longer than is necessary and in line with Prometric's data retention policy.

The following safeguards are applied to the processing of medical data of data subjects:

- Limitations on access to prevent unauthorized consultation, alteration, disclosure or erasure
- Strict time limits for erasure in line with the company's *Records Management Schedule*
- Specific targeted training for those involved in handling medical data
- Logging mechanisms to permit verification of whether and by whom personal data has been consulted, altered, disclosed or erased
- A requirement that medical examinations are undertaken only by authorized occupational health specialists
- Encryption

E. Processing of Personal Data

Prometric processes Personal Data to fulfill requests for information and services, to administer testing programs securely and efficiently, and to operate our business. Specific examples of data processing include:

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 of the test content and results, test scoring, reporting and analysis of results, and customer service related thereto). Where permitted by law,

Prometric may send exam candidates commercial communications and offers for additional testing or training services on behalf of test sponsors.

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. These include payroll and benefits processing, business continuity and disaster recovery planning, to satisfy corporate governance and regulatory obligations, and to control access to secured areas.

  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 Personal Data is limited to individuals inside Prometric on a need to know basis for business purposes and released to persons outside of Prometric only with authorization or as required by law.

3. Legitimate Business Purposes

- Prometric also uses Personal Data as needed to manage everyday business needs such as invoice 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, disaster recovery planning, auditing, reporting and compliance with any legal or regulatory obligations.

F. Monitoring via Digital Video Recording

Prometric deploys Digital Video Recording (DVR or CCTV) throughout its network of test centers and in most corporate offices. This is necessary in order to protect the security of high-stakes proprietary test content, the integrity of the test delivery experience, to deter fraud and cheating, to protect against theft or pilferage, to monitor and restrict secure areas and/or Prometric departments, and for the security of staff and organization property. Access to the recorded material will be strictly limited to authorized personnel. DVR surveillance may be used to manage performance and/or employee disciplinary issues. Please refer to the *DVR Policies and Procedures Operating Guide* for further details.

G. Data Subject Rights

A data subject for whom Prometric processes Personal Data may, at any time:

- request access, rectification, erasure, portability, restriction or objection to their Personal Data;
- make any inquiries, requests or complaints in relation to the use of their Personal Data;
- withdraw consent to the processing of their Personal Data; and

1. Access & Correction

Prometric respects an individual's right to access and correct their Personal Data. Data subjects 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.

Data subjects may request access to their Personal Data and exercise their rights at any time; however, they must supply Prometric with sufficient information to allow us to confirm the identity of the individual making the request for access.

Candidates and employees may even self-correct certain Personal Data 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. Employees may also request to view their personnel file by submitting an email to their Human Resources Business Partner. 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.

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 information is processed solely for research or statistical purposes and does not include Personal Data, 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 business practices, or in future or ongoing negotiations involving the organization.

3. 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 for further advice or instruction.

As permitted by applicable law, data subjects may also withdraw consent to the processing of Personal Data. However, exercising this right may prevent Prometric's ability to deliver any further services or to proceed with legitimate business operations such as the delivery of an exam, compensation and/or benefits administration to name a few.

a. 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.

b. Third-Party Ad Targeting

Prometric will never provide Personal Data to third parties other than for the purpose for which the Personal Data was originally collected. However, for more information about how 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.

H. Compliance with Applicable Data Protection Laws

Prometric complies with all applicable data privacy laws with respect to Personal Data. This includes, but is not limited to, as required, providing disclosures on Prometric processes and procedures related to Personal Data (for example, this Privacy Policy and the statements contained herein), obtaining consent of the individual, adoption of standard contractual clauses with respect to the handling of Personal Data, and/or adherence to local data protection laws in the regions where Prometric conducts business. Where required by law, data subjects will be required to expressly consent to the collection, transfer and processing of their Personal Data.

1. Onward Transfers of Personal Data

Prometric's 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 applicable data protection laws. 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. Additionally, Personal Data that is transferred between our global corporate offices will only be done in furtherance of an authorized and legitimate business purpose. Where required by law Prometric also collects data subject consent through a clear disclosure notice and consent opt-in process in order to transfer Personal Data outside of the region where it was collected. By continuing to provide Prometric with Personal Data or utilize Prometric's services after consent has been obtained a data subject continues to consent to the transfer of Personal Data until such consent is expressly withdrawn in writing.

a. 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/.

b. 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/.

2. Transfer of Personal Data Across Borders

In many instances, the use of third parties will also involve the transfer of personal data across country borders (within the EU / EEA or outside of the EU / EEA). Also, many business processes require the transfer of data within the Company internationally. Specific legal obligations apply when such transfers occur outside the EU / EEA.

When transferring personal data across borders to third parties or internally outside of the EU / EEA:

- Prometric determines if there is a legitimate justification for the transfer of personal data (e.g., valid business reason);
- Prometric follows local legal requirements (e.g. notice to the individual, notification to data protection authorities if necessary, use of contractual safeguards such as EU model clauses).

The transfer of personal data from Prometric operating as controllers in the EEA to other company affiliates established outside the EEA is permitted under the Model Contractual Clauses or other legal mechanisms such as Privacy Shield.

3. 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.

4. 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.

I. 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 done so 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.

J. 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 invite 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.

K. Mobile Applications

Prometric offers mobile aware 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.

We may also offer automatic ("push") notifications. Prometric will provide push notifications only to those data subjects who opt-in to receive such notifications from us. An example includes the identification of impacted employees in the event of a disaster or event of force majeure. No individual 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.

III. Dispute Resolution Process

A. Filing Complaints

Data subjects who have concerns or complaints regarding Prometric's collection and processing of Personal Data are encouraged to first utilize Prometric's internal complaint resolution process by providing a detailed written description of the issue and/or complaint. Test candidates may submit complaints or inquiries by locating the 'Contact Us' tab on Prometric's website and selecting the appropriate link:

https://www.prometric.com/en-us/contact-us/Pages/default.aspx. Employees may submit a complaint or inquiry in writing to their direct supervisor, HR Business Partner, or any member of Prometric's Legal Department.

Prometric will respond to all complaints related to Personal Data issues in forty-five (45) days or less.

Data subjects also have the right to file a complaint directly with the local Supervisory Authority, as relevant under EU data protection law.

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

Candidates also have the right to file a complaint directly with the local Supervisory Authority, as relevant under EU data protection law.

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.
E-mail: ethics@prometric.com
Telephone: 1-888-763-0136

Additional information can be found in the Prometric Code of Business Conduct and Ethics located on the Policy Portal.

Employees also have the right to file a complaint directly with the local Supervisory Authority, as relevant under EU data protection law.

C. EU Data Protection Officer

In compliance with the European Union's General Data Protection Regulation ("GDPR") Prometric has appointed a Data Protection Officer located in the European Union.

Joseph Srouji is the data protection officer for this organization. He is responsible for assisting the organization in monitoring and maintaining compliance with data protection legislation. All employees must co-operate with the data protection officer when carrying out their duties. The data protection officer is also available to answer queries or deal with data subject concerns about Prometric's data protection practices.

Data subjects who feel that the rights afforded to them under GDPR have been violated, or that Prometric is processing Personal Data in violation of GDPR, may submit complaints or inquiries to:

Joseph Srouji
Avocat au Barreau de Paris
Srouji Avocats Selarl
215 rue du Faubourg Saint-Honoré | 75008 Paris l France
joseph.srouji@contractor.prometric.com

Data subjects also have the right to file a complaint directly with the local Supervisory Authority, as relevant under EU data protection law.

D. Additional Recourse Mechanisms under Privacy Shield

With respect to Personal Data of data subjects residing in the European Union and Switzerland, under the EU-US/Swiss-US Privacy Shield Principles 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.

IV. 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.

To submit a request related to your personal data, please click on the link below and complete all of the required fields in the form:
Personal Data Requests

You may also reach us via mail at:

Prometric Privacy Program Manager
Prometric LLC
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.

V. 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.