SYSTEMS AND DATA ACCESS AGREEMENT FOR NON-EMPLOYEES

This Systems and Data Access Agreement for Non-Employees ("Agreement") is effective as of the date the Agreement is acknowledged by You, and is by and between The Prudential Insurance Company of America, including its parent companies and its and their subsidiaries and affiliates ("Prudential"), and You ("You," "Your," and "User"). Definitions for capitalized terms used but not defined herein may be found in the Prudential Policies, linked or attached below.

Prior to being given access to any Prudential Systems or Prudential Data, you must read and accept the terms of this Agreement and any terms attached or linked hereto or otherwise incorporated by reference.

"Prudential Systems" is a term used to encompass broadly any kind of digital communication system used by Prudential. This term is intended to include any new technology, form of communication, or use that may be developed or acquired in the future for digital communications for Prudential business activities. This includes, but is not limited to, the following:

- Prudential-owned or leased computers, desktops, laptops, mobile and other devices;
- Infrastructure such as networks, servers, routers and data storage devices and media;
- Communication systems (including those owned, leased or licensed by Prudential and User's personal devices when used to access or send digital communications or Prudential Information on Prudential Systems) that use software managed by Prudential. Examples of communications include but are not limited to: communications sent through electronic messaging applications, telephone calls, Microsoft Teams' meetings, e-mail and attachments, collaboration tools, instant messages, text messages and social media posts;
- Any environment, application and/or infrastructure, including cloud-based, authorized or provided by Prudential for any purpose, including production, quality assurance or testing.

"**Prudential Data**" shall mean all information and material regarding Prudential or of the entities or persons with whom Prudential does business, including, but not limited to: (i) "Personal Information," which means information provided by or at the direction of Prudential, or to which access was provided in the course of Your providing services to Prudential that identifies an individual (by name, signature, address, telephone number or other unique identifier), or that can be used to authenticate that individual (including, without limitation, passwords or PINs, biometric data, unique identification numbers, answers to security questions, or other personal identifiers); (ii) Prudential trade secrets and proprietary information; (iii) Prudential confidential information; (iv) other information Prudential makes available to You to carry out your job responsibilities; (v) all data, communications, and information sent, received, or stored on Prudential Systems; and (vi) material non public information

You shall comply at all times with Prudential's notices, policies, standards, guidelines, guidance, and procedures for non-employees, set forth herein, attached hereto as Exhibits A, B, & C, and as located at www.prudential.com/links/about/vendor-engagements ("Terms of Engagement Website") (collectively "Prudential Policies"), all as may be supplemented or amended from time to time.

You are responsible for regularly checking for updates and revisions to this Agreement and the Prudential Policies.

You will regard and preserve as confidential all Prudential Systems and Prudential Data. You will not disclose to any person, firm or enterprise, or use for your own benefit or the benefit of any third party, any Prudential Systems or Prudential Data. You further agree to follow applicable laws and Prudential's Policies and standards when provided with access to or use of any Prudential Systems and Prudential Data. Your access or use of any Prudential Systems and Prudential Data is limited to what is necessary for you to provide services to Prudential. You

understand that these obligations continue to exist after termination of your relationship with Prudential. Upon termination of this Agreement, any and all Prudential Systems or Prudential Data in Your possession shall immediately be returned to Prudential, and at Prudential's request, You shall certify that you have so complied with this requirement.

Failure to comply with this Agreement or the Prudential Policies shall constitute a breach of this Agreement and the impacted policy and permits Prudential to immediately terminate Your access to Prudential Systems and Prudential Data. Prudential may also terminate Your access to the Prudential Systems or Prudential Data at any time for any reason and without liability of any kind, including if: (i) your engagement with Prudential terminates; or (ii) it suspects any violation of this Agreement or the Prudential Policies. Prudential's remedies for breach, actual or threatened, are not exclusive and are in addition to any available at law or in equity.

PRUDENTIAL MAKES NO WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO THE PRUDENTIAL SYSTEMS, OR THE USE, ACCURACY OR AVAILABILITY THEREOF. IN NO EVENT SHALL PRUDENTIAL BE LIABLE FOR ANY LOSSES, COSTS, LIABILITIES, OR ANY SPECIAL, CONSEQUENTIAL, INDIRECT, OR OTHER DAMAGES ASSOCIATED WITH OR CAUSED IN ANY WAY BY YOUR ACCESS TO PRUDENTIAL'S SYSTEMS OR DATA, WHETHER IN CONTRACT, TORT, NEGLIGENCE, OR OTHERWISE.

You may not assign or otherwise transfer Your rights or obligations under this Agreement to any third party. This Agreement shall be governed by the laws of the State of New Jersey. You agree to exclusive jurisdiction of any action, dispute, or proceeding arising out of or relating to this Agreement in the United States District Court for the District of New Jersey, Newark Division, or any court of the State of New Jersey sitting in Newark, and you waive, to the fullest extent permitted by law, any objection to these venues and any claim of an inconvenient forum.

Acknowledgment & Consent

I, the undersigned, have read and fully understand the Systems and Data Access Agreement for Non-Employees and its exhibits, and I agree and undertake to be bound by and comply with its terms.

In accordance with the Prudential Policies, I acknowledge that any information sent through or stored on a Prudential System may be subject to access, inspection, monitoring, and/or removal by Prudential, and I consent to such access, monitoring, inspection, and removal by Prudential.

To finalize your acceptance of and agreement to all of the above conditions and acknowledge your receipt of the notices referenced herein, please sign below:

_____

Print Name: _____

Date: _____

Exhibit A
PRUDENTIAL INFORMATION SECURITY REQUIREMENTS

This document outlines the Prudential information security requirements in effect for all Prudential Systems for non-Prudential personnel being provided access to Prudential Systems. These requirements are subject to change by Prudential from time to time.

1. User Responsibilities - an end User is any person who has access to Prudential's Systems. A User's security responsibilities are to:

- Understand his/her responsibility to comply with these requirements and other Prudential Policies, standards, guidelines and procedures regarding information security (whether corporate or business unit owned).
- Report observed or suspected information security violations to his or her Prudential project manager, the appropriate security group and/or the BISO, Operations Control Center, and/or the Information Security Office.
- Maintain the confidentiality of his or her password. A User must not share his/her password, personal identification number (PIN), or token with another person.
- Change his or her password immediately if he or she thinks the password may have been compromised.
- Report any suspected misuse of a User ID or any inappropriate solicitation of a password to his or her Prudential project manager, the appropriate security group, and/or the BISO or the Information Security Office.
- Choose a strong password that can be remembered without writing it down. Never store the password in a login script or programmable device. See Information Security website or discuss with Your Prudential project manager for guidelines on selecting strong passwords.
- Log off or lock a terminal or workstation when leaving it unattended.
- Ensure that only software that has been approved by Prudential's Enterprise Architecture Review Board or other standards bodies within Prudential, and licensed as may be required by the issuers, is installed on his or her workstation, laptop, network, and other parts of Prudential's Systems. Non-approved\unauthorized software includes, but is not limited to, hacking tools, shareware, evaluation software, etc.
- Ensure that computers and other portable office devices (e.g., laptops, smartphones, tablets, USB flash drives, etc.) are either in sight or physically secured at all times.
- Ensure that Corporate-related Security software (patch management, security system management) is not removed, altered, or disabled.
- Ensure that the computer and any portable office devices have a password-protected screen saver or time-out.
- Never connect, install, or configure equipment (including software tools) to the Prudential network without following an approved change control process and obtaining the appropriate authorization(s).
- Ensure the data on computer and other portable devices is adequately protected (hard drive password, encryption, etc.).
- Refrain from knowingly forwarding or circulating external e-mail virus warnings.
- Ensure virus protection on computer is not disabled for any reason.
- Not forward e-mail from Prudential Systems that contains Prudential Data to Your personal e-mail or other non-approved digital communication accounts.

2. PRUDENTIAL SYSTEMS ACCESS (Local and Remote). Prudential Systems access procedures are dependent upon the types of communications services used to connect the site with the Prudential's Data Processing Centers. Regulations regarding access to Prudential Systems are as follow:

- Prudential Systems access instructions/procedures must be kept in a secure locked place at all times when not in use.
- Personal computers used to access Prudential Systems must never connect to the Internet without firewall protection or be connected to a network that does not have Internet firewall protection.
- The User's computer must not be logically connected to two (or more) networks at the same time, when one of those networks is a Prudential network (i.e., the User is not permitted to bridge the two networks).
- Software, instructions, and keys needed to facilitate VPN or other remote connections must be provided on a "need to know" basis only.
- Access to computers that connect to the Prudential remote access Virtual Private Network (VPN) using a Digital Subscriber Line (DSL) or cable modem must be controlled in such a manner that all unsolicited Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) packets from the Internet are blocked. The configuration of the access control device (e.g., personal firewall, Instant Internet) must be approved by the Information Security Office.
- Workstations (including desktops and laptops) must never be left signed on while unattended for any period of time. They must be signed off or locked when not in use.
- All equipment that is located inside a Prudential facility or that connects to the Prudential network as a node must be able to be monitored by Prudential.

3. USER ACCESS. Protection of the Systems is dependent upon the ability to control access to the Systems. It is the User's responsibility to be certain that computer accessibility is properly secured.

- Only those individuals whose duties require it can be provided with access to Prudential's Systems. Each User will be assigned a unique and individual user ID.
- Use of Prudential's Systems must be limited to those Systems for which the User is authorized.
- When a User no longer requires access to a Prudential System, the User must notify Prudential immediately so that user IDs and access can be removed.

4. PASSWORDS/PINS and ACCESS TOKENS. Passwords and access tokens are critical to the security of the Prudential Systems as they verify that anyone signing on has the authority to do so.

- Passwords/PINs must be changed at least every ninety (90) days.
- Passwords must contain at least one alphabetic and one numeric character.
- The minimum length of a password is eight (8) characters. The minimum length of a PIN is four (4) characters.
- Passwords must not be the same as the user ID or contain the user ID.
- A User's new password/PIN cannot be the same as the previous six (6) passwords.
- Passwords/PINs must not be stored in hard copy.
- Passwords/PINs must not be shared.
- Confidentiality of passwords/PINs must be maintained. No operations or support procedure will solicit or require a person to disclose his/her password/PIN to another.
- Passwords/PINs must never be sent in clear text across the network.
- User must not know or attempt to know another User's or a Prudential employee's password/PIN.

- When an access token is used, each User is assigned a unique token (e.g. SecurID card, key fob). Tokens must not be shared and a User must not use or attempt to use another User's access token.
- Tokens must be carried separately from the device used to access Prudential information.
- User must not obtain access to the Prudential Systems for use by any other User or Prudential employee.

5. VIRUS PROTECTION. Anti-virus measures are essential to ensure protection against outside infection. All non-Prudential personnel must familiarize themselves with Prudential anti-virus rules (stated below) and take, at a minimum, the following steps to assure compliance.

- All electronic files introduced into Prudential's distributed computing environment must be scanned before being used. This includes program and executable files, data files, e-mail, e-mail attachments, electronic documents, spreadsheets, etc.
- An approved Prudential anti-virus product using continuous 'on access' scanning must be deployed to minimize User intervention. Scheduled scanning of critical files stored on Intel-based clients and servers must be performed on no less than a weekly basis. Anti-virus protection must be kept current in order to guard against new viruses.
- All virus incidents must be reported to the appropriate Prudential Help Desk.
- Virus warnings must be channeled to the Prudential Help Desk and not distributed informally.
- Virus protection must not be disabled.
- No computer virus may be intentionally introduced to a system except in the Prudential Virus Research Lab, or location designated by the CIO. No one can maintain live viruses for research or any other purposes except the Prudential Anti-virus Coordinator.

Exhibit B

RECORDING NOTICE TO NON-EMPLOYEES

This Recording Notice to Non-Employees (the "Notice") applies to independent contractors, consultants, temporary workers, employees or contractors of a third party ("non-employee") and does not apply to employees, former employees or job applicants of Prudential Financial, Inc. and its subsidiaries and affiliates ("Prudential"). Prudential ("we" or "us") respects your privacy, and we are committed to protecting your personal information. This Notice is designed to inform non employees ("you" or "your") about how we may collect, use, share, retain and disclose personal information collected from you or about you in the context of recorded business meetings, as outlined within the Recording in the Workplace Standards (found in the Digital Communications and Acceptable Use Policy). It also outlines your choices.

How We Collect Personal Information

Business meetings may sometimes be recorded by Prudential to enhance knowledge sharing in a collaborative online environment.

Depending on how the meeting is held, this may include the recording of voice, photo and/or video of the attendees. Information captured during the recording may be considered Personal Information, as defined in the Privacy Notice for Non-Employees and data protection laws. Personal Information in recordings could include images of you (e.g., your webcam footage) or audio of comments you make or content you provide to any chat function.

This Notice augments the Systems and Data Access Agreement for Non-Employees and the Privacy Notice for Non-Employees and explains how the recordings will be used by Prudential. Consistent with applicable law, the legal basis for processing this Personal Information generally is legitimate interest. This applies when the processing is: (i) not required by law but is of a clear benefit to Prudential or the individual, (ii) there is limited privacy impact on you as the individual; and (iii) we think you would reasonably expect us to use the Personal Information in the way that we do. You also always have a choice - If you do not want to be recorded you can mute your microphone, turn off your webcam and/or choose not to attend or to not contribute during the meeting.

How We Use Personal Information

The recordings may be used by Prudential to enable meeting participants and non-attendees to share knowledge within the organization and capture the details of a meeting for use after the meeting is over. The recordings will be used and protected consistent with Prudential's Global Privacy Policy and records retention schedule. The recordings will be hosted in Prudential's environment.

How Recordings Are Accessed

The recordings may be made available via Prudential Systems, such as SharePoint, depending on the purpose of the recording and who needs to have access to it. Recorded meetings should be viewed on approved devices in settings that respect the generally non-public nature of meeting content. Downloading, duplicating or editing a recording may be conducted only in limited circumstances where consistent with job duties.

"Prudential Systems" shall mean broadly any kind of digital communication system used by Prudential. This term is intended to include any new technology, form of communication, or use that may be developed or acquired in the future for digital communications for Prudential business activities. This includes, but is not limited to, the following:

- Prudential-owned or leased computers, desktops, laptops, mobile and other devices;
- Infrastructure such as networks, servers, routers and data storage devices and media;
- Communication systems (including those owned, leased or licensed by Prudential and User's personal devices when used to access or send digital communications or Prudential Information on Prudential Systems) that use software managed by Prudential. Examples of communications include but are not limited to: communications sent through electronic messaging applications, telephone calls, Microsoft Teams' meetings, e-mail and attachments, collaboration tools, instant messages, text messages and social media posts;
- Any environment, application and/or infrastructure, including cloud-based, authorized or provided by Prudential for any purpose, including production, quality assurance or testing.

Changes to this Notice

Prudential reserves the right to modify, add or remove portions of this notice at any time. If we decide to change this notice, we will post the updated Notice on the Prudential Vendor Code of Conduct and Terms of Engagement site found at www.prudential.com/links/about/vendor-engagements.

Contact Us

If you have further questions or concerns regarding the recording, or if you wish to exercise your individual rights, if available under applicable law, relating to the recording, please contact the Global Privacy Office at global.privacy@prudential.com.

Exhibit C

Prudential Financial, Inc.

Personal Information Protection Notice for Non-Employees

Last Updated: April 2024

Contents

About This Notice 9

What Information About You We Collect, Use, Transfer and Disclose, and Why 9

Types of Personal Information We May Collect, Use, Transfer and Disclose 10

Legal Basis for Processing Personal Information 12

How We Use Personal Information 13

Categories Of Unaffiliated Third Parties with Which PFI Shares Personal Information 14

Other Sources from Whom We Receive Personal Information 15

Transfers Of Personal Information 15

Data Security and Integrity 16

Your Rights 16

Your Obligations 17

Updates To This Notice 18

Retention 18

Contact Information and Complaints 18

Additional Jurisdictional Information 18

- Additional Information Regarding the UK and EEA 18
- Additional Information for California Residents 19
- Additional Information for Other Jurisdictions 19

About This Notice

This Privacy Notice for Non-Employees (the "**Notice**") applies to independent contractors, consultants, temporary workers, and employees or contractors of any third-party (together, "**non-employee**") working for Prudential Financial, Inc. or its subsidiaries and affiliated entities (together, "**PFI**"). This Notice does not apply to PFI employees, former employees, or job applicants.

Some of the countries in which PFI operates have laws related to the collection, use, transfer, and disclosure of Personal Information of individuals, including our non-employees. We take these obligations very seriously, and we are committed to protecting the privacy of our current and former non-employees. The purpose of this Notice, as well as any applicable jurisdictional addendums, is to give you information about what Personal Information we collect, use, transfer and disclose because of the services you provide, including as described in PFI's contract or other relationship directly with you or with your employer, and to inform you about the rights and choices you may have.

What Information About You We Collect, Use, Transfer and Disclose, and Why

Throughout your relationship with PFI, we may have collected or will collect information about you and your working relationship with us. Additionally, we may collect information, as needed, about your spouse, domestic/civil partner, or dependents ("**Dependents**"). We refer to such information as "Personal Information." For more specific information regarding what Personal Information about you that we may collect, use, transfer and disclose, please see the **Types of Personal Information We May Collect, Use, Transfer and Disclose** section of this Notice. Policies, standards, handbooks, work rules, office manuals, and notices provided in your local office may provide additional details.

We collect and process information about you for a variety of reasons. For more detail regarding the purposes for which we process Personal Information, please see the **How We Use Personal Information** section of this Notice. Where none of these reasons apply, your decision to provide Personal Information to PFI is voluntary. If we collect or process Personal Information based on your consent, you may withdraw your consent at any time.

We receive Personal Information from you as well as from other sources. Please see the **Other Sources from Whom We Receive Personal Information** section of this Notice for more details.

We may combine Personal Information obtained through the sources referred to in this Notice with other information. Where we do so, we will treat the combined information as Personal Information if the resulting combination may be used to reasonably identify or locate you in the same manner as Personal Information alone.

We may anonymize and aggregate your Personal Information so that it does not reasonably identify you as an individual. Once anonymized - and provided it may not be combined with other information we hold to reasonably identify you - we may use it for any purpose.

Transfer And Joint Use of Personal Information

Due to the global nature of PFI's operations, we disclose Personal Information to personnel and departments in PFI subsidiaries and affiliates worldwide to fulfill the purposes described in this Notice. This may include transferring Personal Information to other countries (including countries other than where you are based and that have a different data protection regime than is found in the country where you are based). For those located in the European Economic Area (the "EEA"), we may transfer your Personal Information to countries located outside of the EEA. For more information on the transfer of Personal Information, please see the Transfers of Personal Information section of this Notice.

Access to Personal Information within PFI will be limited to those who have a need to know the information for the purposes for which we collect and use it (please see the How We Use Personal Information section of this Notice), and may include your managers within PFI and their designees, personnel in IT, Compliance, Legal, Finance and Accounting, and Internal Audit.

All personnel within PFI, including both PFI employees and non-employees, will generally have access to your business contact information, such as your name, position, business unit, telephone number, postal address, email address and name of the individual(s) at PFI who may oversee the project on which you are working as part of the services you are providing to PFI, as well as your supervisor or manager as designated by your employer.

From time to time, PFI will need to make Personal Information available to other unaffiliated third parties. Please see the Categories of Unaffiliated Third Parties with Whom PFI Shares Personal Information section of this Notice for a list of the categories of unaffiliated third parties. Some of the unaffiliated third parties will be located outside of your home area, including in the United States and elsewhere.

Types of Personal Information We May Collect, Use, Transfer and Disclose

During your professional relationship with us, we may collect the following types of Personal Information about you:

- **Personal Details:** Name, employee identification numbers that your employer may provide or that we may assign to you, work and home contact details (email, phone numbers (including mobile), fax numbers, physical address) language(s) spoken, gender, age, date of birth, biometric data, national/government identification number, tax identification number, marital/civil partnership status, spouse or domestic partners, dependents, disability status, emergency contact information, nationality, personal financial records (including securities account numbers, current account holdings and trading activity), photographs, and CCTV images.

- **Documentation Required under Immigration Laws:** Citizenship, passport or visa data, details of residency or work permit.

- **Compensation:** Depending on whether PFI is paying your employer directly or whether you are providing services to PFI as an independent contractor, PFI may need to collect information related to your fees associated with services you are providing, which may also require you to provide PFI with basic tax documentation (W-9 or equivalent) in order for PFI to compensate you for the products and / or services you provide. Depending on the way PFI is compensating you for the products and / or

services you provide, you may also need to provide PFI with your banking details, bank account number, tax identification number and related information, tax location code, and working time records (hours worked).

- **Position:** Description of the current position you hold with your employer or your role as an independent contractor, job title, job function(s) and subfunction(s), company name and code, legal employer entity, branch/unit/department name and code, location, employment status and type, full-time/part-time, terms of employment with your employer or as an independent contractor, and your reporting manager(s) information.

- **Resource Planning Information:** Details contained in your resume/CV (previous employment background, education history, professional qualifications, language and other relevant skills, certifications, certification expiration dates), employment history, information necessary to complete a background check, where applicable, professional licenses or certifications held, training and development programs planned, attended and completed that are relevant to the services you provide to PFI, web-based training programs, and driver's license information (if relevant to the services you will provide to PFI).

- **Business-related Travel & Expenses, Gifts and Entertainment:** Travel and transaction details for business-related travel, including travel reservation numbers, if issued; expense reimbursement information, credit card numbers and transactions; travel information (airline, flight number, hotel name, dates of travel); gifts given or received, including description of gift, reason for giving/receiving gift, and value; meals or entertainment given or received, including type, value, location, and reason for giving such gift/meal/entertainment.

- **Investigation Records:** Name, position, and contact information of any employee making a complaint against you, the individuals who are subjects of the complaint or an investigation, and the information documented from the individuals interviewed during the investigation, persons investigating the complaint, the facts collected, and the results of the investigation.

- **System and Application Access Data:** Information required to access PFI systems and applications such as System ID, LAN ID, XID, email account, instant messaging account, mainframe ID, system passwords, branch state, country code, previous branch details, and previous department details, and electronic content produced by you (which may include, for example, data collected when you swipe your badge to enter Prudential buildings, print from managed devices, or use a technology kiosk) using PFI systems.

- **Use of Systems:** Any use, including (1) communications sent or received through PFI systems, including incoming and outgoing emails, instant messaging, text messages, and alternative messaging systems (business and personal); (2) community and social media postings; (3) internet history and sites accessed on PFI devices or platforms; (4) logs regarding use of systems and applications; and (5) keystroke recording.

- **Use of PFI Websites:** Your use of PFI's publicly facing websites or PFI social media may result in the collection of Personal Information. To the extent applicable, the collection and use of Personal Information from a PFI publicly facing website or social media is described in the applicable website's online privacy statement.

- **Biometric Data and Audio/Visual Data:** Biometric data, such as your fingerprints, voice prints / voice recordings, photo / video (through your participation in recorded events), and facial recognition.

- **Sensitive Personal Information:** We also collect certain types of sensitive information only when permitted by applicable law, such as health/medical information (may include COVID-19 vaccination status and responses to health-related questions asked in connection with pandemic-related screening), place of birth, trade union membership information, immigration/citizenship status, religion, and race or ethnicity. We collect this information for specific purposes, such as health/medical information to accommodate a disability or illness and to provide benefits; religion or church affiliation in countries such as Germany where required for statutory tax deductions; and diversity-related Personal Information (such as gender, race, or ethnicity) to comply with legal obligations and internal policies relating to diversity and antidiscrimination. Please be assured that, as explained in the following section, we will only use such sensitive information for the following purposes and as provided by law.

The provision of Personal Information as described in this Notice is partly a statutory requirement and may also be a contractual requirement under your contract with PFI. In general, you are required to provide such Personal Information, except in limited instances when we indicate that the provision of certain information is voluntary (e.g., in connection with a personnel satisfaction survey).

In some instances, the provision of the Sensitive Information listed above is voluntary. We will let you know when that is the case, and if you decide not to share voluntary Sensitive Information withholding that information will not impact your relationship with us.

Legal Basis for Processing Personal Information

Data protection law seeks to ensure that the way your Personal Information is used is fair and lawful. Some countries require that we have a legal justification for using your Personal Information. To comply with the law, we need to tell you the legal justifications for our processing of your Personal Information. These justifications vary based on where you are located. PFI relies on the following legal grounds for the collection, processing, and use of your Personal Information:

- **When Pursuing Legitimate Interests.** We process Personal Information for our legitimate interests in conducting and managing our business as a global organization; for example: (1) to ensure that our networks and information are secure; (2) to administer and conduct business across the organization; and (3) to prevent fraud;

- **With Your Consent (or express/explicit consent for sensitive personal information)**. As permitted by applicable law and where appropriate, provided that such consent is voluntary, you have the right to withdraw your consent at any time, and your consent meets applicable legal requirements of such consent;

- **When We Have Legal Obligations.** We will process your Personal Information when we have a legal obligation to do so (e.g., responding to a legal process or enforceable government request) or for our own compliance with legal obligations, including by not limited to social security and protection law, data protection law, tax law, and corporate compliance laws;

- **To Perform a Contract with You.** We will process your Personal Information when processing is necessary for the execution or performance of a contract with you; and

- **Protection of the Vital Interests** – To protect your life or health, or the life and health of another individual.

Additional legal justifications may also be available in the country in which you are based, and we may also rely on these justifications from time to time.

How We Use Personal Information

In addition to the use cases that may be detailed elsewhere in this Notice, we use your Personal Information listed above for the following business purposes associated with the administration of your relationship with PFI:

- **Service Level Metrics:** Reviewing and evaluating the services you provide to PFI, which may include service performance management, administration and reviews, processing accounts payable and receivable, honoring other contractual benefits (e.g., service level incentives), providing accommodations, performing background checks (where permitted by law), managing grievances or complaints regarding the services you provide.

- **Analytics:** Planning, projecting, managing, and enhancing data security. For instance, we use analytics to assist in service succession planning, to ensure business continuity, and to identify patterns in the use of technology systems, as well as to protect PFI's people and property.

- **Communications and Emergencies:** Facilitating communication with you, ensuring business continuity, property management (e.g., laptops and mobile phones), providing references, protecting your health and safety along with the health and safety of our employees, and others, safeguarding IT infrastructure, office equipment and other property, and facilitating communication with you and your nominated contacts in cases of emergency.

- **Business Operations:** Operating and managing the IT and communications systems (including email collection, storage and review), managing product and service development, improving products and services, managing PFI assets, operating and managing facilities, allocating PFI assets and human resources, performing strategic planning, facilitating project management, ensuring business continuity, compiling of audit trails and other reporting tools, maintaining records relating to business activities, budgeting, financial management/reporting and communications, and managing mergers, acquisitions, sales, reorganizations or disposals and integration with purchaser.

- **Compliance:** Complying with legal and other requirements such as income tax and national insurance deductions, record-keeping and reporting obligations, conducting audits, compliance with government inspections and other requests from government or other public authorities, responding to legal process requests such as subpoenas, pursuing legal rights and remedies, defending litigation and managing any internal complaints or claims, conducting investigations including reporting of allegations of wrongdoing, policy violations, fraud, or financial reporting concerns, and complying with internal policies and procedures.

- **Monitoring Use of Technology:** Reviewing internet access and monitoring of internet history and sites accessed on PFI Systems; monitoring use of information resources including applications, communications tools, and connected devices; monitoring incoming and outgoing text messages on PFI Systems and social media postings; monitoring of telephone conversations on PFI Systems; monitoring incoming and outgoing email messages on PFI Systems. We monitor usage of technologies and contents of communications to protect PFI and to detect, respond to, and prevent crime, fraud, other illegal activities, and violations of our policies and procedures. Our monitoring of your use of PFI Systems is described in the Digital Communications and Acceptable Use Policy (and related Standard) previously or otherwise known as the Digital Communications and Internet Use Policy (and related Standard) which can be found on PFI's PolicyHub, on the Prudential Supplier Code of Conduct and Terms of Engagement Page, or available upon request.

- **Marketing Products and Services:** PFI may use your Personal Information to send you marketing communications on PFI products and services or products and services offered by third parties that PFI or its Affiliates are licensed to sell. Please visit the Privacy Center on Prudential.com to learn about your choices regarding receiving marketing communications from PFI.

We only use your Sensitive Personal Information to administer your relationship with us (e.g., for workplace accommodations), to maintain sickness/medical leave information and records, to comply with applicable health regulations, to monitor for equal opportunities in the workplace, and to comply with any other statutory obligations.

Categories Of Unaffiliated Third Parties with Which PFI Shares Personal Information

We may disclose all categories of Personal Information listed above to the following parties:

- **Professional Advisors:** Accountants, auditors, lawyers, insurers, bankers, and other outside professional advisors where PFI operates.

- **Service Providers:** Consultants, vendors and third- party service providers (including outsourcing partners) that help us provide, support and maintain our business and that may include providing services to you, such as payroll, training, expense management, financial services, travel services, IT systems suppliers and support, credit card companies, medical or health practitioners, trade bodies and associations or providing services (including research and statistics) to us that are helpful to our evaluation of issues impacting staffing resources. In some cases, PFI may provide vendors and service providers with your Personal Information; in other cases, the consultants, vendors, and service providers may collect your Personal Information directly from you on PFI's behalf, and if permitted to do so, may share that Personal Information with PFI.

- **Public and Governmental Authorities:** Entities that regulate or have jurisdiction over PFI, such as governmental authorities, public bodies, judicial bodies, or law enforcement agencies; by a court order; under the discovery process in litigation, investigations, and prosecutions; or in response to requests from, or if required by, government agencies and/or regulators and/or tax advisers, legal advisers, investigators, accountants, financial advisers and/or any other person having appropriate legal authority or justification for receipt of the same. PFI may also disclose Personal Information voluntarily to cooperate with law enforcement agencies or any of the above bodies, including but not limited to

matters of national security, criminal acts, civil claims or as may otherwise be permitted by applicable law.

- **Corporate Transaction:** A third party in connection with any proposed or actual reorganization, merger, sale, joint venture, assignment, transfer or other disposition of all or any portion of PFI business, assets, or stock (including in connection with any bankruptcy or similar proceedings).

Other Sources from Whom We Receive Personal Information

Other than receiving Personal Information directly from you, we generally collect Personal Information from the following sources:

- Your employer;
- PFI employees alongside whom you may work;
- References you provide;
- Clients you service;
- Your family members and dependents (e.g., parents or guardians may be contacted in relation to your relationship with PFI regarding any matter related to that relationship if you are under 18 years of age);
- Third Parties, including but not limited to:
    - Law enforcement agencies, government agencies, regulators and/or any other person having appropriate legal authority (e.g., in the context of requests or investigations where our assistance is required);
    - Previous employers who provide references to PFI;
    - Companies offering employment professional/staffing-related services (e.g., headhunters, recruitment agencies);
    - Credit reference agencies or background check providers (if relevant to your role);
    - Publicly available social media;
    - Educational institutions and membership or certification organizations; and
    - Other sources at your direction.

Transfers Of Personal Information

Personal Information may be transferred to other countries (including countries other than where you are based that have a different data protection regime than is found in the country where you are based). In such circumstances, we will take appropriate steps to provide an adequate level of data protection within the meaning of applicable data protection law, including by implementing the EU Standard Contractual

Clauses, the UK Addendum to the EU Standard Contractual Clauses, or any other appropriate safeguard based on jurisdiction where required. You can request a copy of the appropriate safeguards referenced in this section by contacting us.

A list of the affiliate companies that may jointly process your Personal Information is available in our securities disclosures, including our 10-K → https://www.investor.prudential.com/financials/sec-filings/sec-filings-details/default.aspx?FilingId=15581928, and/or upon request (please refer to the Contact Information and Complaints section of this Notice).

Data Security and Integrity

PFI will take appropriate measures to protect Personal Information that are consistent with applicable privacy and data security laws and regulations, including requiring service providers to use appropriate measures to protect the confidentiality and security of Personal Information. This may include use of security monitoring tools to protect the PFI infrastructure, networks and data.

PFI will take reasonable steps to ensure that the Personal Information processed is reliable for its intended use and is accurate and complete for carrying out the purposes described in this Notice.

Your Rights

If you have any questions or would like to execute your privacy rights as permitted by applicable law, please contact your local Privacy Officer, or use one of the options noted in the Contact Information and Complaints section of this Notice. We will respond to your request consistent with applicable law. Please note, however, that certain Personal Information may be exempt from requests pursuant to applicable data protection laws or other laws and regulations.

You may have specific rights with respect to your Personal Information in certain circumstances depending on your jurisdiction and applicable data protection laws These rights are described below:

- **Right of access:** You may have the right to request a copy of the Personal Information held about you.
- **Right to correct:** You may be entitled to have any inaccurate or incomplete Personal Information held about you corrected or amended.
- **Right to erasure:** You may have the right to have your Personal Information erased (also referred to as the 'right to be forgotten') where, for example, retaining your Personal Information is no longer necessary in relation to your relationship with PFI for which it was originally collected/processed, or where you have withdrawn consent, subject to there being no overriding legitimate interest or legal requirement related to retention for continuing to hold your Personal Information.
- **Right to be informed:** You may have the right to know what Personal Information relating to you is held and processed by us. On receipt of a written request from you, we will provide information relating to the type of Personal Information held, the purposes for which the Personal Information is held or processed and to whom the information is disclosed.
- **Right to restrict processing:** You are entitled at any time to request in writing to discontinue or "block" the processing of your Personal Information where, for example, you believe your Personal

Information is not accurate. Your request should clearly state the reason, and we will respond to your request within a reasonable timeframe detailing whether we are able to comply with the request or the extent to which we are able to comply.

- **Right to object:** We are committed to the legitimate privacy interests of all persons about whom we collect Personal Information, and we do not use Personal Information collected and processed in the context of your relationship with us for profiling, direct marketing, or research purposes. If at any point in time you do not believe this to be the case, you are entitled to object in writing, clearly stating the reasons for your objection. We will seek to make reasonable accommodations in response to your objection, where appropriate and as required.

- **Rights in relation to automated decision-making:** With respect to the collection, processing, and evaluation of Personal Information, subject to any supplementary notice or later amendment to this notice, we do not apply automated decision-making processes, i.e., significant decisions about you are not made based solely on automated processing of your Personal Information.

- **Right to data portability:** You may have the right to request that we provide you with your Personal Information in a structured, commonly used, machine-readable form which provides the ability to move, copy or transfer your Personal Information.
- **Right to anonymization:** You may have the right to have unnecessary, excessive, or non-compliant Personal Information anonymized, blocked, or erased.
- **Right of non-discrimination/retaliation:** We do not discriminate against individuals who exercise any of their rights described in this Notice, nor do we retaliate against individuals who exercise their rights.

For your protection, we may only implement requests with respect to the information associated with the email address that you use to send us your request, and we may need to verify your identity before implementing your request. We will try to comply with your request as soon as reasonably practicable. Please note that certain Personal Information may be exempt from these rights pursuant to local data protection laws.

Your Obligations

Please keep your Personal Information up to date and inform us of any significant changes to your Personal Information. You agree to inform your Dependents whose Personal Information you provide to PFI about the content of this Notice, and to obtain their consent (provided they are legally competent to give consent) for the use (including transfer and disclosure) of that Personal Information by PFI as set out in this Notice. You further agree to follow applicable law and PFI's policies, standards and procedures that are brought to your attention when handling any Personal Information to which you have access in the course of your relationship with us. You will not access, use, or disclose any Personal Information for any purpose other than in connection with and to the extent necessary for your work with PFI. You agree to promptly, and pursuant with your agreement with PFI, raise any potential or actual issues related to privacy to your Privacy Officer or the Global Privacy Office. You understand that these obligations continue to exist after termination of your relationship with PFI.

Updates To This Notice

We may update this Notice to reflect changes in the way we process Personal Information. We will notify you about such changes in the way we use your Personal Information in compliance with applicable law. You can determine when the Notice was revised by referring to the "Last Updated" legend on the top of this Notice.

Retention

We will retain Personal Information for the period necessary to fulfill the purposes outlined in this Notice unless a longer retention period is required or permitted by law. We use the criteria below to determine retention periods for Personal Information:

- The duration of your relationship with PFI;
- As long as we have an ongoing relationship with you or your Dependents;
- As required by a legal obligation to which we are subject;
- So long as the purpose for which the information was collected remains; and
- As advisable considering our legal position (such as in regard of applicable statutes of limitations, litigation, or regulatory investigations).

Contact Information and Complaints

If you have any questions about this Notice or our privacy practices, or concerns about how PFI processes Personal Information, please contact your local Privacy Officer. Alternatively, you can:

- Email the applicable privacy mailbox (global.privacy@prudential.com or pgim.privacy@pgim.com);
- Call the Data Subject Access Request (DSAR) helpline at +1-844-PRU-DSAR (+1-844-778-3727); or
- Complete a DSAR request online at (https://www.prudential.com/links/privacy-center/data-requests).

You always have the right to lodge a complaint with a Data Protection Authority for your country or region or in the place of the alleged misconduct.

Additional Jurisdictional Information

Additional Information Regarding the UK and EEA

- The contact information for our data protection officer (DPO) in Germany is as follows: Jochen Geck VIVACIS Consulting GmbH Horexstraße 1 | ALTER GÜTERBAHNHOF D – 61352 Bad Homburg, Telephone: +49 160 938 492 30, Email: jochen.geck@vivacis.de

- You may lodge a complaint with an EU/EEA or the UK data protection authority for your country or region where you have your habitual residence or place of work or where an alleged infringement of applicable data protection law occurs. A list of data protection authorities in the EU/EEA is available at: (https://edpb.europa.eu/about-edpb/about-edpb/members_en) and information regarding lodging a complaint with the UK ICO can be found here: (https://ico.org.uk/make-a-complaint).

Additional Information for California Residents

In addition to this Notice and the contents herein, if you are a California resident, please refer to the California Resident Privacy Statement, available on the Prudential (https://www.prudential.com/links/privacy-center) and PGIM (https://www.pgim.com/terms-use/privacy-center) privacy centers as well as in PolicyHub, for more information on our privacy practices, including the categories of Personal Information we collect, the purposes for that collection, and our retention practices.

Additional Information for Other Jurisdictions

If your relevant jurisdiction (e.g., your country of residence) has specific privacy requirements that have not been addressed by the content of this Notice, a supplemental addendum to this Notice may be available. The jurisdictional addendum, along with this Notice, details PFIs processes and practices in place to address the privacy rights of individuals from that jurisdiction.