

GIC Personal Data Protection Policy

This Personal Data Protection Policy informs you of how GIC Private Limited and its subsidiaries, all overseas offices and relevant investment holding / management services companies (collectively, “GIC Group”), as well as its representatives and/or agents (collectively referred to herein as “GIC”, “the Group”, “us”, “we” or “our”) manage your Personal Data (defined below).

Please take a moment to read this Personal Data Protection Policy so that you know and understand the purposes for which we collect, use and disclose your Personal Data.

Depending on the country in which your Personal Data is being collected, used, disclosed or processed by us, different country-specific addendum* may apply. If your Personal Data has been collected, used or disclosed by us in a particular country, you should check if there is a country-specific addendum applicable to you and the terms of the collection, use, disclosure and processing of your Personal Data. The terms set out in such addendums are in addition to the terms set out in this Personal Data Protection Policy and form an integral part of this Personal Data Protection Policy.

The security of your Personal Data is important to us. We have taken reasonable steps to safeguard the Personal Data under our control against unauthorised access, disclosures and other similar risks. Access to your Personal Data is restricted to those parties who need to know such Personal Data in relation to the purposes specified in this Personal Data Protection Policy.

By interacting with us including through electronic mail message or phone conversations, accessing and using GIC websites, intranet or portal or submitting information to us, you agree and consent to us collecting, using, disclosing and sharing amongst ourselves your Personal Data, and disclosing such Personal Data to GIC’s authorised service providers and relevant third parties in the manner set forth in this Personal Data Protection Policy.

If you do not agree to this Personal Data Protection Policy, please do not access or use GIC websites, intranet or portal.

***Note:** There is no country-specific addendum for Singapore.

This Personal Data Protection Policy supplements but does not supersede nor replace any other consents you may have previously provided to GIC in respect of your Personal Data. Your consents herein are additional to any rights which any member of the GIC Group may have at law to collect, use, disclose or process your Personal Data.

GIC may update or change this Personal Data Protection Policy from time to time to ensure that it is consistent with our future developments, industry trends and/or any changes in legal or regulatory requirements. All changes will be posted on this page.

Subject to your rights at law, you agree to be bound by the prevailing terms of this Personal Data Protection Policy as updated from time to time on this website. Please check back regularly for updated information on the handling of your Personal Data.

This Personal Data Protection Policy was last updated on 15 Feb 2023.

QUICK LINKS TO ADDENDUMS

1. [Australia Addendum](#)
2. [Brazil Addendum](#)
3. [China Addendum](#)
4. [India Addendum](#)
5. [Japan Addendum](#)
6. [Korea Addendum](#)
7. [UK Addendum](#)
8. [US Addendum](#)

1. Personal Data

- 1.1 In this Personal Data Protection Policy, “Personal Data” shall mean the following (unless otherwise defined in the country-specific addendums):

- (a) Personal Information, being any data, whether true or not, about an individual who can be identified (i) from such data; or (ii) from such data and other information to which we have or are likely to have access, including data in our records as may be updated from time to time;

Examples of such Personal Information you may provide to us include (depending on the nature of your interaction with us) your name, NRIC, passport or other identification number, telephone number(s), mailing address, email address, facial biometric information and any other information relating to either yourself or any other individuals which you have provided us in any forms you may have submitted to us, or via other forms of interaction with you;

- (b) information other than Personal Information submitted by you to us via GIC websites, intranet or infrastructure as indicated in the respective country addendum.

2. Collection of Personal Data

- 2.1 Generally, we collect Personal Data in the following ways:

- (a) when you register and login to our career website;
- (b) when you submit forms or applications to us;
- (c) when you submit your resumes and/or CVs to us;
- (d) when you submit queries, requests, complaints or feedback to us;
- (e) when you respond to our request for additional Personal Data;
- (f) when you ask to be included in an email or other mailing list;
- (g) when a recruitment agency refers your resume to us;
- (h) when you respond to our initiatives or contact us;
- (i) when you browse our intranet or other websites;
- (j) when you take part in events organised solely or jointly by GIC and/or any third parties;

- (k) when you are employed or engaged by GIC; and/or
 - (l) when you provide information (including biometric information) to GIC for access control or security purposes; and/or
 - (m) when you register to be a part of our alumni network; and/or
 - (n) when you submit your Personal Data to us for any other reasons.
- 2.2 If you provide us with any Personal Data relating to a third party (e.g. information of your dependents, spouse, children and/or parents), by submitting such information to us, you represent and warrant to us that they have read and understood this Personal Data Protection Policy and that you have obtained the requisite consent of such third party and/or are authorized to provide us with such Personal Data for the relevant purposes contained in this Personal Data Protection Policy.
- 2.3 You are to ensure that all Personal Data submitted to us is complete, accurate, true and correct. Failure on your part to do so may result in our inability to fulfil your requests and/or applications or delays in processing your applications.
- 2.4 When you browse GIC websites, intranet or portal, you generally do so anonymously but please see paragraph 5 below for information on cookies and other technologies which we have implemented on GIC websites, intranet or portal.

3. Purposes for the Collection, Use, Disclosure and Processing of Your Personal Data

- 3.1 GIC generally collects, uses, discloses and processes your Personal Data for the following purposes:
- (a) responding to your queries and requests and complaints;
 - (b) managing the infrastructure and business operations of GIC and complying with internal policies and procedures, including providing you with access and/or use of websites, systems and infrastructure (including but not limited to processing CCTV records, office access logs and enabling biometric identifiers);
 - (c) managing our alumni programme and/or corporate social responsibility projects;
 - (d) facilitating investments, business asset transactions (which may include but is not limited to any merger, acquisition or asset sale) and business agreements with counterparties;
 - (e) matching any Personal Data we hold which relates to you for any of the purposes listed herein;
 - (f) verifying your identity and conducting background checks, to the extent permissible by law, and due diligence;
 - (g) conducting data analytics for the purpose of (i) system and process improvements, (ii) risk/fraud management, (iii) regulatory and compliance risk management, (iv) investment insights and (v) enhancements to human resources processes;
 - (h) dispute resolution, preventing, detecting and investigating non-compliance with laws, regulations, and internal corporate policies, including fraud and financial crimes, analysing and managing other commercial risks and risks arising from GIC's operations and investment activities;

- (i) protecting and enforcing our contractual and legal rights and obligations;
- (j) conducting audits, reviews and analysis of our internal processes;
- (k) fulfilling GIC's legal, contractual or regulatory obligations, including complying with any applicable laws, regulations, rules, codes of practice or guidelines or to assist in law enforcement and investigations by relevant authorities; and/or
- (l) purposes reasonably related to any of the above.

3.2 **In addition**, GIC may collect, use and / or disclose your Personal Data for the following purposes, depending on the nature of our relationship with you:

- (a) if you are a job applicant:
 - (i) verifying and processing your personal particulars, processing your application, evaluating your suitability, eligibility or qualification for employment with GIC as well as assessing your financial status;
 - (ii) communicating with you to inform you of changes and developments to GIC's policies, terms and conditions and other administrative information;
 - (iii) sending you updates and alerts related to job applications which you may have requested for;
 - (iv) conducting market research for statistical, profiling and statistical analysis for the improvement of services provided to you; and/or
 - (v) purposes reasonably related to any of the above.
- (b) if you are an employee, officer or owner of an external service provider or vendor:
 - (i) verifying and processing your personal particulars and assessing your organisation's and/or your suitability, eligibility or qualification as an external service provider or vendor for GIC as well as your organisation's and your financial status;
 - (ii) communicating with you to inform you of changes and developments to GIC's policies, terms and conditions and other administrative information;
 - (iii) managing project tenders and quotations, processing orders or managing the supply of goods and services;
 - (iv) creating and maintaining profiles of our service providers and vendors in our system database;
 - (v) processing and payment of vendor invoices and bills; and/or
 - (vi) purposes reasonably related to any of the above.
- (c) if you are an employee, officer or owner of our investment counterparties, including our joint venture partners, brokers, investee companies etc.:
 - (i) verifying and processing your personal particulars to maintain accurate records;
 - (ii) communicating with you to inform you of changes and developments to GIC's policies, terms and conditions and other administrative information;

(iii) creating and maintaining profiles of our investment counterparties in our system database; and/or

(iv) purposes reasonably related to any of the above.

3.3 Furthermore, where permitted under applicable law, if you attend events organised by GIC or jointly by GIC and third parties, photographs and/or video recordings may be taken at events which you have attended, and used and disclosed for our marketing and/or promotional purposes. Such photographs and videos may be published on our website, social media channels or made publicly available to recipients overseas for our marketing and/or promotional purposes.

4. Disclosure and/or Transfer of Personal Data

4.1 GIC will take reasonable steps to protect your Personal Data against unauthorised disclosure. Subject to the provisions of any applicable law, your Personal Data may be disclosed to the parties listed below (whether located in your local jurisdiction or overseas), for the purposes listed above (where applicable) to:

- (a) other entities within GIC;
- (b) insurance companies and brokers in connection with staff insurance;
- (c) recruitment agencies;
- (d) agents, contractors or third party service providers who provide operational services to GIC, such as courier services, telecommunications, information technology, advertising, payment, payroll, processing, training, market research, storage, archival, customer support, marketing and social media partners in relation to marketing and/or promotional photographs and videos published on our website, social media channels or otherwise made publicly available to recipients overseas, investigation services or other services to GIC;
- (e) any business partner, investor, assignee or transferee (actual or prospective) to facilitate business asset transactions (which may extend to any mergers, acquisitions and debt or asset sale);
- (f) local and overseas financial institutions and their respective service providers;
- (g) our professional advisers such as our consultants, auditors and lawyers;
- (h) trade unions[#];
- (i) business and charity partners in relation to events planning;
- (j) relevant government regulators, government ministries, statutory boards, embassies, or authorities and/or law enforcement agencies, whether local or overseas, to comply with any directions, laws, regulations, rules, codes of practice or guidelines, or schemes issued or administered by any of them;
- (k) other organisations which may request that we provide them with your Personal Data for evaluative purposes; and/or
- (l) any other party to whom you authorise us to disclose your Personal Data.

[#]Note: This is not applicable to the India and UK Addendum.

5. Use of Cookies, Web Beacons, and Similar Technologies on the Website

- 5.1 When you visit, access or interact with GIC websites, intranet or portal and use our services, we or our authorized service providers may use cookies, web beacons, and other similar technologies for collecting and storing information to help provide you with a better, faster, and safer web experience.
- 5.2 The information collected by us or our authorised service providers may recognise a visitor as a unique user and may collect information such as how a visitor arrives at our websites, what kind of browser a visitor is on, what operating system a visitor is using, a visitor's IP address and a visitor's click stream information and time stamp (for example, which pages they have viewed, the time the pages were accessed and the time spent per web page).
- 5.3 The use of cookies, web beacons and similar technologies by us on our website perform different functions. They are either necessary for the functioning of our services, help us improve our performance, or serve to provide you with extra functionalities.

Cookies – Small text files (typically made up of letters and numbers) placed in the memory of your browser or device when you visit a website or view a message. Cookies allow a website to recognize a particular device or browser. There are several types of cookies:

- Session cookies expire at the end of your browser session and allow us to link your actions during that particular browser session.
- Persistent cookies are stored on your device in between browser sessions, allowing us to remember your preferences or actions across multiple sites.
- First-party cookies are set by the site you are visiting
- Third-party cookies are set by a third party site separate from the site you are visiting.

Cookies can be disabled or removed by tools that are available in most commercial browsers. The preferences for each browser you use will need to be selected separately and different browsers offer different functionalities and options.

Web beacons - Small graphic images (also known as “pixel tags” or “clear GIFs”) may be included on our websites and services. Web beacons typically work in conjunction with cookies to profile each unique user and user behaviour.

Similar technologies – Technologies that store information in your browser or device utilizing local shared objects or local storage, such as flash cookies, HTML 5 cookies, and other web application software methods. These technologies can operate across all of your browsers.

- 5.4 We offer certain website features and services that are available only through the use of these technologies. You are always free to block, delete, or disable these technologies if your browser so permits.
- 5.5 However, if you decline cookies or other similar technologies, you may not be able to take advantage of certain website features or services tools. For more information on how you can block, delete, or disable these technologies, please review your browser settings. You may refer to the Cookie Policy on our website for detailed information on the cookies we use, as well as the purposes for which we use such cookies.

6. Use of Anonymised Information

- 6.1 From time to time, we may aggregate and anonymise Personal Data and send this aggregated, anonymised data to our authorised service providers for the purposes of statistical studies and service improvement relating to GIC websites, intranet or portal, and for purposes reasonably related thereto.

7. Contacting Us – Withdrawal of Consent, Access and Correction of your Personal Data

- 7.1 If you:

- (a) have any questions or feedback relating to your Personal Data or our Personal Data Protection Policy;
- (b) would like to withdraw your consent to any use of your Personal Data as set out in this Personal Data Protection Policy; or
- (c) would like to obtain access or make corrections to your Personal Data, please contact any of the following:

Name: Lynn Hew Ooi Lyn

Email: lynnhew@gic.com.sg

Contact number: +65-68898377

Department: Legal and Compliance Department

Group Email: GrpLCD_PersonalData@gic.com.sg

- 7.2 If you withdraw your consent to any or all use of your Personal Data, depending on the nature of your request, GIC may not be in a position to administer or comply with the relevant contractual agreement or arrangement in place. This may also adversely impact and affect your employment relationship or other agreements or arrangements with GIC. GIC's legal rights and remedies in such event are expressly reserved.

8. Governing Law

- 8.1 This Personal Data Protection Policy shall be governed in all respects by the laws of Singapore.

Australia Addendum

This addendum to the Personal Data Protection Policy applies to you if your personal information (within the meaning defined in this Addendum) is collected, used, held or disclosed by us in Australia and is governed by the Privacy Act 1988 (Cth) and the Australian Privacy Principles (Privacy Laws).

Where there is an inconsistency between the terms of the Personal Data Protection Policy and the terms of this Australia Addendum, the terms of this Australia Addendum override the Personal Data Protection Policy. **Quick guide to contents**

1. What is your “personal information”?
2. What kinds of personal information do we collect from you?
3. How do we hold your personal information?
4. For what purposes do we collect, hold, use and disclose your personal information?
5. Who do we disclose your personal information to?
6. Overseas recipients
7. How to access and correct your personal information
8. Feedback and complaints
9. Contact us

1. What is your “personal information”?

Personal information is information or an opinion about you where you are identified, or can reasonably be identified, whether or not that information or opinion is true or recorded in a material form.

Personal information also includes **sensitive information**, which is information or opinion about your racial or ethnic origin, political opinions/ associations, religious beliefs or affiliations, philosophical beliefs, membership of trade/professional associations or a trade union, sexual orientation or practices, or criminal record that is also personal information, as well as health information, generic information, biometric information used for the purpose of automated verification or identification and biometric templates.

2. What kinds of personal information do we collect from you?

Personal information Most of the time we will collect your personal information directly from you, when you apply for our products or services, use our website, applications, enter our promotions, provide products or services to us or apply for a job from us.

Sometimes we will collect your personal information from someone else. If this is the case, we will take reasonable steps to ensure that person makes you aware of how we manage your personal information.

The kinds of personal information that we may collect about you include:

- **(identity information)** your full name, date of birth, and other government identifiers used to verify your information (such as your driver's licence or passport number).
- **(contact details)** your address, telephone number and email address.
- **(financial information)** your bank account information, income, assets and liability information, and financial statements.
- **(our interactions with you)** your history of transactions and interactions with us including timing and the content of any details you provided in updates, additional information, providing feedback or raising a complaint.
- **(job applications)** if you apply for a job with us and are not successful, we may keep records about candidacy including your application, education qualifications and background checks.
- **(online behavioural data)** we may collect your IP address, browser type, operating system, referring URLs, information on actions taken on our websites, and dates and times of visits.
- **(social media and websites)** if we release articles or materials on social media platforms, we may collect your information from your comments, responses or 'likes'. We may also collect your personal information from you automatically when you browse GIC's websites, intranet or portal (including through cookies).
- **(audio and visual data)** your image may be collected if you visit our offices and audio recordings if you call us.

Sensitive information

The kinds of sensitive information that we may collect about you include your criminal history should we complete background checks on you if you apply for a job with us, or if you disclose your health or ethnic origin information to us.

We may also collect biometric information through facial recognition technology and create biometric templates for access control and security purposes.

We will not collect your sensitive information without obtaining your consent before or at the time of collecting it.

Other information

We may also collect your Tax File Number. If we do, we will comply with the Privacy (Tax File Number) Rule 2015.

You may choose not to provide certain information however, if you choose not to, we may not be able to fulfil your requests, process your application or provide you with the products or services that you have requested.

Where we have collected unsolicited personal information, we may destroy or de-identify the information (if it is reasonable and lawful to do so) after assessing whether we have grounds to collect that information.

3. How do we hold your personal information?

We may hold your personal information in:

- **(physical records)** our physical, hard copy (paper) files in our office or access restricted storage.
- **(electronic records)** our computer systems, data bases, secured servers, cloud storage and the IT servers that may be located outside Australia.
- **(information technology)** we use encryption techniques to convey your personal data between you and our servers. We also protect our network servers using firewalls.
- **(personnel controls)** only certain staff members are authorised to access data containing your personal information. The authorised staff are required to comply with our additional obligations under an internal code on personal data confidentiality.

The security of your personal information is important to us. We have taken reasonable steps to safeguard the personal information under our control against unauthorised access, disclosures and other similar risks. Access to your personal information is restricted to those parties who need to know such personal information in relation to the purposes specified in this Addendum.

4. For what purposes do we collect, hold, use and disclose your personal information?

We collect, use and hold your personal information for a number of purposes, including those set out in section 3 of the main body of the GIC Personal Data Protection policy.

5. Who do we disclose your personal information to?

Any personal information which we collect about you may be used by us for the purposes explained in the section above, or for any reasonably related purposes.

We may disclose your personal information to the list of parties set out in section 4 of the main body of the GIC Personal Data Protection policy.

6. Overseas recipients

We may disclose your information overseas, including countries where GIC has operations (such as Singapore, Brazil, China, India, Japan, Korea, the United States or the United Kingdom), or countries where GIC has investments or receives outsourced services. If we do this, we make sure there are arrangements commensurate to the Australian privacy laws in place to protect your information.

If you have provided your consent to us disclosing your personal information to overseas recipients without complying with APP 8.1, to the extent allowed by the APP, we may disclose your information to overseas recipients without taking reasonable steps to ensure the overseas recipient does not breach the APPs.

7. How to access and correct your personal information

You have the right to ask to access and correct the personal information that we hold about you. If you would like us to provide access or a correction, we recommend that you:

- contact us on the details below under 'Contact us' and set out the details of your access or correction request, including the manner you would like to access the information you are requesting access;
- comply with any requests we may have to verify your identity or the authority of your third-party representative (if you have one); and

- allow us 30 days to respond to your request. Our response will detail our reasons for approving or denying your request.

Certain access requests may incur a charge for our reasonable administrative costs to retrieve your personal information. No charge will be imposed for a request to correct your personal information.

If you contact us to withdraw consent to any use of your personal information in accordance with section 7(b) of the Personal Data Protection Policy, we will comply with the request if we are legally required to do so or if we no longer require the personal information for a purpose permitted by the Privacy Laws, but we may continue to hold, use or disclose some personal information if required or permitted to do so under the Privacy Laws or other laws.

If you are unhappy with the outcome of your request, you may provide us with feedback or raise a complaint as explained under 'Feedback and complaints'.

8. **Feedback and complaints**

If you have any feedback or wish to raise a complaint about how your Personal Information was managed, including our compliance with the APPs, please contact us using the details found under the 'Contact us' section.

We will use our best endeavours to respond to your complaint within 14 days. However, where the matter is complex, we will write to you and advise you that we may respond within 30 days.

If you are dissatisfied with the outcome of your complaint, you may have the complaint reviewed externally by the Office of the Australian Information Commissioner, whose details are set out below:

| Office of the Australian Information Commissioner | |
|----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| By post: | GPO Box 5218, SYDNEY NSW 2001 |
| By telephone: | 1300 363 992 (10am to 4pm AEST, Monday to Thursday) |
| By online form: | www.oaic.gov.au/privacy/privacy-complaints/lodge-a-privacy-complaint-with-us |
| Website: | www.oaic.gov.au |

9. **Contact us**

For requests for access or correct, other enquiries about how we manage your personal information, including questions about this Privacy Policy, please contact us on the details below:

| GIC Australia Privacy Officer | |
|--------------------------------------|------------------------------------------------------------------------------------|
| Contact: | Lynn Hew Ooi Lyn (located in Singapore) |
| By post: | Suite 17.01, Level 17, Chifley Tower, 2 Chifley Square, Sydney NSW 2000, Australia |
| By telephone: | +65-68898377 |
| By email: | lynnhew@gic.com.sg |

Brazil Addendum

This addendum to the Personal Data Protection Policy applies to you if your Personal Data is being collected, used, disclosed or processed by us in Brazil. The terms set out in this Brazil Addendum are in addition to the terms set out in the Personal Data Protection Policy and form an integral part of the Personal Data Protection Policy. In the event of any conflict or inconsistency between the Personal Data Protection Policy and the terms of this Brazil Addendum, this Brazil Addendum shall govern and prevail.

1. Protection of Personal Data

- 1.1 We will at all times keep your Personal Data confidential, unless we are required to disclose such Personal Data by court order.
- 1.2 The security of your Personal Data is important to us. We have adopted reasonable security practices and procedures to safeguard the Personal Data under our control against unauthorised access, disclosures and other similar risks. Access to your Personal Data is restricted to those parties who need to know such Personal Data in relation to the purposes specified in this Personal Data Protection Policy.
- 1.3 Whilst we will endeavour to take all reasonable and appropriate steps to keep secure any Personal Data under our control, you acknowledge and agree that we cannot provide any absolute guarantees regarding the security of your Personal Data.

China Addendum

(Last updated on **29 July 2022**)

This addendum to the Personal Data Protection Policy applies to you if your Personal Data is being collected, used, disclosed or processed by us in China. The terms set out in this China Addendum are in addition to the terms set out in the Personal Data Protection Policy and form an integral part of the Personal Data Protection Policy. In the event of any conflict or inconsistency between the Personal Data Protection Policy and the terms of this China Addendum, this China Addendum shall govern and prevail.

1. Categories of Personal Data to be Processed and the Corresponding Purposes

1.1 In general, we may collect and process your Personal Data in the following scenarios :

- (a) **when you submit queries, requests, complaints or feedback to us**, we will collect your name, contact details and the other information provided by you to respond to your queries, requests, complaints or feedback.
- (b) **when you ask to be included in an email or other mailing list**, we will collect your name, email address and contact details.
- (c) **when you take part in events organised solely or jointly by GIC and/or any third parties**, we may also collect, use, disclose and transfer photos and videos featuring you for publicity purposes on GIC's external and internal webpages, brochures and other electronic medium such as social media sites and emails.
- (d) **when you browse our intranet or other websites**, we will collect information such as how a visitor arrives at our websites, what kind of browser a visitor is on, what operating system a visitor is using, a visitor's IP address and a visitor's click stream information and time stamp (for example, which pages they have viewed, the time the pages were accessed and the time spent per page) to provide you with a better, faster and safer web experience.

1.2 If you are a job applicant, we may collect and process your Personal Data in the following scenarios:

- (a) **when you apply for job positions in GIC or your resume is referred by recruitment agencies**, we will collect the following information that you provide in your application process:
 - i. CV;
 - ii. Name, email address, contact numbers, address, graduation year and student status, employment history, educational history, professional certificates, language skills, current/ last drawn compensation details, expected compensation, previous employment/ internship record with GIC, details of any relatives/ acquaintances/ friends working in GIC, criminal/ dismissal record, character referee details.
- (b) **when you are employed or engaged by GIC**, we will collect the following categories of personal data, in addition to those set out in 1.2(a) above:
 - i. date of birth, beneficiary details, family members' date of birth, rental home address (for local hire expats who are claiming tax free rental); and
 - ii. personal data as set out in 1.5 below.

to manage, evaluate or terminate your employment relationship with us and other purposes reasonably related to the employment relationship (including for example workforce planning, processing your payroll and tax matters, conducting appraisals and performance management, processing medical claims, administering benefits which apply to you and your family, facilitating the organisation of events for current and former staff, employee mobility and relocation, carrying out administrative and support processes and publishing articles / photographs on GIC's intranet).

Job applicants, vendors, members of the public and investment counterparties

- 1.3 If you are an employee, officer or owner of an external service provider or vendor, **when you or your organization provides services to us**, we may collect your name and contact details (email and mobile number), qualification and experience, and reference check details to assess your organisation's and/or your suitability, eligibility or qualification as an external service provider or vendor for GIC as well as your organisation's and your financial status, and to make the payment to your organization.
- 1.4 If you are an employee, officer or owner of our investment counterparties, including our joint venture partners, brokers, investee companies etc., **when you or your organization establishes business cooperation with us**, we may collect your name, date of birth, address and contact details to maintain accurate records, and bank account information relating to funding- related issues that we have to process.
- 1.5 Certain Personal Data processed by us are Sensitive Personal Data under Chinese data protection laws, such as those set out below. These are collected by us for the purpose of recruitment, payroll and benefits processing, or providing you with access to premises, or in the case of our business partners, for payments for investment funding purposes. If you do not provide such information to us, we cannot achieve the relevant processing purposes.
- i. ID / Passport number;
 - ii. Bank account details;
 - iii. Declaration of health issues (when completing enrolment of group term insurance);
 - iv. Family member's ID if they enroll onto GIC's medical insurance;
 - v. Criminal records;
 - vi. Facial biometric information (if you opt-in to using facial verification to enter our premises in mainland China).

2. **Entrusted Processing and Sharing of Personal Data**

- 2.1 In order to improve the efficiency of information processing, we may engage other entities within GIC and third parties (such as recruitment, payment, payroll, training and other HR service providers, telecommunication service providers, IT service providers, investigation service providers, professional advisers, local and overseas financial institutions and their respective service providers) to process your Personal Data on our behalf. We will enter into strict confidentiality agreements with such third parties and require them to process Personal Data in accordance with our requirements and the confidentiality and security measures required by laws and regulations.
- 2.2 Your Personal Data may be disclosed to the parties listed below for the corresponding purposes:
- (a) **when you are employed or engaged by GIC**, we will provide certain categories of Personal Data to **certain parties** for the purpose of processing employment-related issues for you. Please refer to our Employee Personal Data Protection Policy for detailed information.
 - (b) In the event of **any change, merger, acquisition, reorganization, or liquidation** involving the transfer of Personal Data, we will ask the new company or organization holding your Personal Data to continue to process your Personal Data in accordance with this Personal Data Protection Policy. If the new company or organization needs to use your Personal Data for purposes not stated in this Personal Data Protection Policy, they will obtain your consent in accordance with the applicable laws and regulations.
 - (c) to the **competent domestic or foreign law enforcement body, regulatory, government agency, court or other third party** where we believe that such disclosure is to (1) comply with an applicable law or regulation; (2) exercise, establish or defend our legal rights; or (3) protect your vital interests or those of any other person.
- 2.3 Your Personal Data in sections 1 & 2 above may be disclosed to the head office of GIC in Singapore for the corresponding purposes set out in this Personal Data Protection Policy (you may exercise your data subject rights by contacting the recipient in the manner set out in section 6 below).

3. **Protection of your Personal Data**

- 3.1 The security of your Personal Data is important to us. We have adopted reasonable security practices and procedures to safeguard the Personal Data under our control against unauthorised access, disclosures and other similar risks. Access to your Personal Data is restricted to those parties who need to know such Personal Data in relation to the purposes specified in this Personal Data Protection Policy.

4. **Storage of your Personal Data**

- 4.1 **Location of Storage:** Generally, we will store your Personal Data in Singapore. However, as GIC is a multinational company, for the purposes specified in this Personal Data Protection Policy, we may transfer your Personal Data to other countries in accordance with the applicable data protection laws and regulations.
- 4.2 **Retention Period:** We may retain your Personal Data only for as long as it is necessary for the purposes it has been collected and as required by applicable law. Where we no longer require your Personal Data for those purposes, we will delete or anonymize such Personal Data in accordance with our internal Record Retention policy.

5. **Your rights**

- 5.1 You are conferred by the applicable data protection laws with the following data subject rights. If you want to exercise any of such rights, you can contact us using the contact details provided in "Contact Us".
- (a) **Right of access.** You are entitled to a copy of the Personal Data we hold about you and to learn details about how we process it. We may require you to prove your identity before providing the requested information.
 - (b) **Right to rectification.** We take reasonable steps to ensure that the information we hold about you is accurate and complete. However, if you believe this is not the case, you have the right to request that any incomplete or inaccurate Personal Data that we process about you is amended.
 - (c) **Right to deletion.** You have the right to ask us to delete your Personal Data, for example where the Personal Data we collected is no longer necessary for the original purpose, where the Personal Data has become obsolete or where you withdraw your consent (if we are processing your Personal Data based on your consent). However, this will need to be balanced against other factors. For example, we may not be able to comply with your request due to certain legal or regulatory obligations.
 - (d) **Right to restriction of processing.** You are entitled to ask us to stop using your Personal Data.
 - (e) **Right to data portability.** You have the right to ask us to transfer your Personal Data that you have provided to us to a third party of your choice. This right can only be exercised in certain circumstances as provided by Chinese laws.
 - (f) **Right to withdraw consent.** We may ask for your consent to process your Personal Data in specific cases. When we do this, you have the right to withdraw your consent at any time. We will stop the further processing as soon as possible after the withdrawal of your consent. However, this does not affect the lawfulness of the processing before consent was withdrawn.
- 5.2 We will respond to your requests of exercising your data subject rights in accordance with the applicable data protection laws. To the extent permitted by laws and regulations, we may not be able to respond to your request of exercising your rights in the following circumstances:
- (a) If your request is contrary to our obligations under laws and regulations;
 - (b) If the requested data is directly related to national security or national defense security;

Job applicants, vendors, members of the public and investment counterparties

- (c) If the requested data is directly related to public safety, public health, or significant public interest;
- (d) If the requested data is directly related to criminal investigations, prosecutions, trials and enforcement of judgments, etc.;
- (e) If we have sufficient evidence of your subjective malice or abuse of rights;
- (f) If it is in the interest of safeguarding your or other individuals' significant legitimate rights and interests, such as life and property, but it is difficult to obtain your authorization or consent;
- (g) If responding to your request to exercise your rights would result in serious harm to your or other individuals' or organizations' legitimate interests;
- (h) If the requested data involves trade secrets.

6. Contact Us

- 6.1 If you have any questions or concerns about this Policy or your Personal Data held by us, especially if you consider that our processing your Personal Data impairs your legitimate interests, please contact us at through the means below . We will review your query without delay and respond timely according to the applicable laws and regulations.

Email: GrpLCD_PersonalData@gic.com.sg

Call: +65 6889 8888

7. Transfer of Personal Data

- 7.1 You consent to us transferring all or any of your Personal Data to the parties specified in this Personal Data Protection Policy (whether located in China or overseas) for the purposes specified in this Personal Data Protection Policy (where applicable).

India Addendum

(last updated 15 February 2023)

This addendum to the Personal Data Protection Policy applies to you if your Personal Data is being collected, used, disclosed or processed by us in India. The terms set out in this India Addendum are in addition to the terms set out in the Personal Data Protection Policy and form an integral part of the Personal Data Protection Policy. In the event of any conflict or inconsistency between the Personal Data Protection Policy and the terms of this India Addendum, this India Addendum shall govern and prevail.

1. Personal Data

1.1 For the purposes of this India Addendum, references to “Personal Data” in the Personal Data Protection Policy and this India Addendum shall be read to mean “Sensitive Personal Data”.

1.2 The Personal Data which we may collect about you are the following:

Personal identifiers:

- (a) Name;
- (b) Birthdate;
- (c) Passwords;
- (d) Email address; and
- (e) Biometric information.

Banking information:

- (a) Bank account information; and
- (b) Other financial information such as credit information and claims information.

Background verification information:

- (a) Criminal activities records, court records, and police records;
- (b) Declarations regarding financial standing; and
- (c) Employment, education history and references through CV.

Health related information:

- (a) Pre-employment medical check report (collected from our vendor clinic); and
- (b) Medical records and history.

1.3 The legal basis for processing your Personal Data are the following:

- (a) Consent;
- (b) Except in the case of Sensitive Personal Data, where processing is necessary for:
 - (i) recruitment or termination of employment;
 - (ii) provision of any service to, or benefit sought by an employee;
 - (iii) verifying attendance of an employee; or

- (iv) any other activity relating to the assessment of the performance of an employee;
and
- (c) Under any law for the time being in force made by the Parliament or any State Legislature, or for compliance with any order or judgment of any court or tribunal in India.

Please note that we may process your Personal Data for more than one lawful ground depending on the specific purpose for which we are using your Personal Data.

2. Transfer of Personal Data

- 2.1 You consent to us transferring all or any of your Personal Data to the parties specified in this Personal Data Protection Policy (whether located in India or overseas) for the purposes specified in this Personal Data Protection Policy (where applicable). In case of any cross-border transfer of your Personal Data (including Sensitive Personal Data), we will ensure compliance with applicable laws in India in relation to such transfer.
- 2.2 You acknowledge that some countries to which we may transfer your Personal Data may not have data protection laws which are as stringent as the data protection laws of India. You acknowledge and agree that it is adequate that when we transfer your Personal Data to any other entity overseas, we will put in place contractual obligations on the transferee which will oblige the transferee to adhere to the same levels of data protection which are adopted by us.

3. Retention of Personal Data

- 3.1 We will retain your Personal Data for as long as reasonably necessary to fulfil the purposes for which we have collected it. We may retain your Personal Data for a longer period by obtaining your explicit consent or for complying with a legal obligation.

4. Protection of Personal Data

- 4.1 The security of your Personal Data is important to us. We have adopted reasonable security practices and procedures to safeguard the Personal Data under our control against unauthorised access, disclosures and other similar risks. Access to your Personal Data is restricted to those parties who need to know such Personal Data in relation to the purposes specified in this Personal Data Protection Policy.
- 4.2 Whilst we will endeavour to take all reasonable and appropriate steps to keep secure any Personal Data under our control, you acknowledge and agree that we cannot provide any absolute assurance regarding the security of your Personal Data.

5. Your Rights

Subject to certain conditions, you have the following rights in relation to your Personal Data:

- 5.1 **Access and Confirmation:** You have the right to obtain the following:

- (a) confirmation whether we are processing or have processed your Personal Data;
- (b) access to the Personal Data provided by you, or any summary thereof; and
- (c) a brief summary of processing activities undertaken with respect to your Personal Data. In this regard, you have the right to access in one place the identities of the entities with whom your Personal Data has been shared, along with the categories of Personal Data shared with them.

- 5.2 **Correction and Erasure:** You have the right to request for:

- (a) the correction of inaccurate or misleading Personal Data;
- (b) the completion of incomplete Personal Data;
- (c) the updating of Personal Data that is out-of-date; and
- (d) the erasure of Personal Data which is no longer necessary for the purpose for which it was processed.

In case your request under this Clause 5.2 is rejected, we will provide you adequate justification in writing for rejecting the application. If you do not agree with our decision, you have the right to require us to take reasonable steps to indicate, alongside your Personal Data, that the same is disputed by you. In case your request under this Clause 5.2 is accepted, we will also take necessary steps to notify all relevant entities or individuals to whom such Personal Data may have been disclosed regarding the relevant correction, completion, update or erasure, particularly where such action may have an impact on your rights and interests or on decisions made regarding you.

- 5.3 **Data Portability:** Where the processing of Personal Data has been carried out through automated means, you have the right to receive the following Personal Data in a structured, commonly used and machine-readable format:

- (a) the Personal Data provided by you;
- (b) the data which has been generated in the course of your employment; or
- (c) the data which forms part of your profile or which we have otherwise obtained.

You can also request for your Personal Data transferred to any other entity in the same format.

You will not be entitled to exercise your rights under this Clause 5.3 if (a) the processing of your Personal Data is necessary for functions of a governmental authority or in compliance of law or order of a court or, (b) if complying with your request would reveal a trade secret of another entity or person or would not be technically feasible.

- 5.4 **Consent Withdrawal:** You have the right to withdraw your consent at any time in writing by sending an e-mail to us at GrpLCD_PersonalData@gic.com.sg , in accordance with the terms of this Policy. However, please note that withdrawal of consent will not be retrospective in nature and shall be applicable prospectively. In case you do not provide your Personal Data or consent or subsequently withdraw your consent, we may not be able to carry out certain employment related functions for which the said information was sought.

- 5.5 **General Conditions:** For exercising any right under this Clause 5, other than Clause 5.5 below, you are required to make a request in writing to us either directly or through a consent manager with the necessary information as regards your identity. We will acknowledge the receipt of such request and communicate our response within such period as specified by provisions of applicable law. If we refuse your request, we will provide our reasons for the same in writing. Please note that we are not obliged to comply with your request under this Clause, where such compliance will harm the legal rights of another person. For complying with your request for exercising any right under this Clause 5, other than Clause 5.5 below, we may charge such fee as specified by provisions of applicable law, other than for requests relating to Clauses 5.1(a) and 5.1(b) and Clause 5.2, which will be free of charge.

- 5.6 **Restrict or prevent continuing disclosure:** By an order of a competent adjudicating officer based on an application made in compliance with the provisions of law, you can request us to restrict or prevent the continuing disclosure of your Personal Data where such disclosure:

- (a) has served the purpose for which it was collected or is no longer necessary for the purpose;
- (b) was made with your consent and you have withdrawn such consent; or
- (c) was made contrary to the provisions of any law.

6. Contacting Us – Exercising Your Rights

- 6.1 In order to exercise the rights above and those granted to you in the main Personal Data Protection Policy, please contact the Grievance Officer at the contact details set out below. The same shall be considered in accordance with the procedures and timelines mentioned under applicable laws of India.
- 6.2 If you withdraw your consent to any or all use of your Personal Data, depending on the nature of your request, GIC may not be in a position to administer any contractual relationship in place. Depending on the situation, this may also result in the termination of your employment, agreement and/or any other forms of arrangement with GIC. GIC's legal rights and remedies in such event are expressly reserved. You may withdraw your consent by contacting the Personal Data team at GrpLCD_PersonalData@gic.com.sg.

7. Grievance Officer

- 7.1 We have appointed a Grievance Officer to address any concerns or grievances that you may have regarding any use of your Personal Data. If you have any such grievances, please write to our Grievance Officer and the Personal Data team at: GrpLCD_PersonalData@gic.com.sg.
- 7.2 You also have the right to file a complaint with the relevant data protection authority in accordance with the provisions of applicable law.

Japan Addendum

(last updated 29 March 2022)

This addendum to the Personal Data Protection Policy applies to you if your Personal Data is being collected, used, disclosed or processed by us in Japan. The terms set out in this Japan Addendum are in addition to the terms set out in the Personal Data Protection Policy and form an integral part of the Personal Data Protection Policy. In the event of any conflict or inconsistency between the Personal Data Protection Policy and the terms of this Japan Addendum, this Japan Addendum shall govern and prevail.

1. Personal Data

- 1.1 For the purposes of this Japan Addendum, references to “Personal Data ” in the Personal Data Protection Policy and this Japan Addendum shall, in addition to the definition set out in the main Personal Data Protection Policy, also be read to include: (1) any “Personal Identification Code”, which refers to any biometric data that identifies a specific individual, or any code uniquely assigned to an individual with respect to the receipt of goods or services, or instruments with which to purchase such goods or services, as defined in the Act on the Protection of Personal Information (Act No. 65 of 2015) (“PIPA”) Article 2, Paragraph 2; and (2) “Sensitive Information”, which means sensitive personal information or special care-required personal information, as defined in PIPA Article 2, Paragraph 3. Both defined terms (1) and (2) above are more fully defined in Annex A attached hereto.

2. Compliance with Laws

- 2.1 GIC (Japan) K.K. (“JPO”) shall comply with the PIPA.

3. Appropriate Acquisition and Use of Personal Data

- 3.1 JPO shall acquire and use Personal Data in an appropriate and fair manner.

4. Organizational Structure Concerning Personal Data

- 4.1 JPO shall internally develop adequate organizational structure to ensure appropriate handling of Personal Data under its control by setting up or conducting the basic policy, the internal rules, the safety management measures in connection with organizational matters, personnel, facilities and appliances, and technical matters, and the external regulatory environment research, and shall respond as promptly as possible to the requests for disclosure and correction, and other inquiries received from the individuals whose Personal Data is held by us, regarding these matters.

5. Sensitive Personal Information

GIC Group may acquire Sensitive Personal Information and provide the same to third parties identified in the Data Protection Privacy Policy including this Japan Addendum for the purposes of use set forth in Paragraph 6.2 below.

6. Publicly Announced Matters Regarding Personal Data

6.1 Name, address, and name of representative of the operator handling Personal Data

GIC (Japan) K.K.

17th Floor, Pacific Century Place, Marunouchi, 1-11-1, Marunouchi, Chiyoda-ku, Tokyo, Japan

Ken Sugimoto, Representative Director

6.2 Purpose of use of Personal Data

- (1) Personal Data in general

In addition to the purposes stated in the Personal Data Protection Policy Paragraph 3.1 and 3.2, JPO uses Personal Data for the following purposes:

- (a) Creation of staff register, business communication, procedures in relation to benefit packages and social insurance, and other legally required procedures;
- (b) Determination and payment of salary, bonus, retirement allowance, other benefits, etc., and withholding tax procedures;
- (c) Performance evaluation, decision of promotion/demotion, personnel transfer (including intercompany transfer) and decision of posting destination;
- (d) Education and training, and health care for employees, etc., official commendation/sanctions and implementation of other rules of JPO and that of GIC Pte Ltd;
- (e) Outsourcing purposes, including but not limited to, receiving cloud services from a cloud data processor or subprocessor including those located outside Japan, such as (i) setting up, operating, monitoring and otherwise receiving the cloud service for human resource personal data processing, (ii) technical support, (iii) consulting services, and (iv) communication with authorised users.

(2) Individual number (also known as “My Number”)

JPO shall use individual numbers (as provided for in the Act on the Use of Numbers to Identify a Specific Individual in Administrative Procedures) of its employees and their dependents for the purposes below:

- (a) Process related to withholding tax that is implemented by an employer under the Income Tax Act;
- (b) Process related to individual residence tax that is implemented by an employer under the Local Tax Act;
- (c) Process related to employment insurance that is implemented by an employer under the Employment Insurance Act;
- (d) Process related to health insurance that is implemented by an employer under the Health Insurance Act (application/payment);
- (e) Process related to employees’ pension insurance that is implemented by an employer under the Employees’ Pension Insurance Act (application);
- (f) Process related to industrial accident insurance that is implemented by an employer under the Industrial Accident Compensation Insurance Act;
- (g) Any process related to (a) through (f) above as well as the purposes of use indicated under Paragraph (1) and section 3.1 and 3.2 of the main policy.

6.3 Joint use

JPO shall jointly use Personal Data with joint users as follows:

(1) Personal Data items for joint use

- (a) Business title, location, grade, compensation, working schedule, education level, history of internal moves and other employment contract details.
- (b) Names, contact details, addresses, date of birth, marital status, gender, religion, nationality, citizenship, dependent information, passport information, details of military service (if applicable), next-of-kin details, work union membership, national insurance number or other social security details, banking information, employee ID, photos and other employment identification details, pay grade, job code, salary information, benefit election information, number and value of stock rights, educational history and employment history, travel details, corporate card number, bank details, external directorships (if any), employment satisfaction related information, performance information, photographs, videos and information necessary in relation to legal proceedings (whether prospective, pending or current), for obtaining legal advice, or otherwise for establishing, exercising or defending legal rights, which may include Personal Data.

(2) Scope of joint users

GIC Group (i.e., GIC Pte. Ltd. and any and all affiliated companies of GIC Pte. Ltd.) (whether located in Japan or overseas as listed on GIC's website)

(3) Purpose of joint users

- (a) Planning and providing the services to GIC Group entities;
- (b) Employment management, allocation of human resources, business communications, etc. and
- (c) Any and all purposes described in Paragraph 6.2 above

(4) Administrator of Personal Data for joint use

GIC (Japan) K.K.

17th Floor, Pacific Century Place, Marunouchi, 1-11-1, Marunouchi, Chiyoda-ku, Tokyo, Japan

Ken Sugimoto, Representative Director

6.4 **Contact for complaints**

Please address any complaints regarding JPO's handling of Personal Data to the contact set forth in Paragraph 8.1 below.

7. **Transfer of Personal Data**

- 7.1 You consent to us transferring all or any of your Personal Data to the parties specified in this Personal Data Protection Policy (whether located in Japan or overseas) for the purposes specified in this Personal Data Protection Policy (where applicable).
- 7.2 JPO shall provide all of the Personal Data under its control, in order to manage such information in the cloud, to cloud operators in countries which GIC Pte.Ltd. selects by reasonably considering that legislation thereof has been adequately developed for protection of Personal Data or put in place arrangements to ensure the Personal Data will be adequately protected.

- 7.3 You acknowledge and agree that some countries to which we may transfer your Personal Data may not have data protection laws which are as stringent as the data protection laws of Japan. You acknowledge and agree that it is adequate that when we transfer your Personal Data to any other entity overseas, we will put in place contractual obligations on the transferee which will oblige the transferee to adhere to the same levels of data protection which are adopted by us.

8. Disclosure, Correction, Suspension of use or Deletion of your Personal Data

- 8.1 If you have any complaints regarding JPO's handling of Personal Data or would like to request the disclosure, correction, suspension of use, deletion of your Personal Data (subject to our rights at law), please contact the following personnel of GIC Pte Ltd. A reasonable amount of fee may be charged for each disclosure request, in consideration of the amount of actual out-of-pocket expenses incurred by GIC:

Name: Lynn Hew Ooi Lyn

Email: lynnhew@gic.com.sg

Contact number: +65-68898377

- 8.2 No request for disclosure shall be accepted in any of the following cases where:

- (a) JPO cannot confirm either identification of the relevant principal individual who requested the disclosure or his/her authorized proxy;
- (b) JPO does not possess the Personal Data the disclosure of which was requested;
- (c) The disclosure may damage life, body, property or other right and interest of the relevant individual or a third party;
- (d) The disclosure may significantly disturb appropriate implementation of JPO's business operations; or
- (e) The disclosure violates any other laws and regulations.

In such cases, JPO will send a notification with the reason for non-disclosure.

9. Exemptions

The provision of the Personal Data Protection Policy Clause 6 does not apply to Personal Data used by JPO.

ANNEX A to Japan Addendum

Definitions of “Individual Identification Code” and “Sensitive Personal Information”

“Individual Identification Code” means (i) any code into which a distinguishing body part of an individual has been converted so that it may be processed by a computer and which can identify the relevant individual: or (ii) any code allocated to an individual for the purchase or use of goods or services, or that is entered or recorded on cards or other documents issued to an individual, as specified by the applicable Cabinet Order (PIPA Article 2, Paragraph 2).

The Cabinet Order specifies Individual Identification Code such as code data regarding DNA base sequence, facies, iris pattern, voice print, gait, hand and finger veins, and fingerprints, as well as passport number, pension beneficiary number, driver's license number, residential certificate code, individual number so called “My Number”, national welfare and health insurance beneficiary number, welfare and health insurance beneficiary numbers under other Japanese special laws, membership certificate numbers of specified associations formed under Japanese special laws, employment insurance beneficiary number under the employment insurance law, and special permanent residential certificate number issued under Japanese special law regarding the immigration control of persons who renounced the Japanese nationality based on the peace treaty with Japan. (PIPA Enforcement Order Article 1, Paragraph 1).

“Sensitive Personal Information” means the following information:

- (1) Race (PIPA Article 2, Paragraph 3);
- (2) Creed (PIPA Article 2, Paragraph 3);
- (3) Social status (PIPA Article 2, Paragraph 3);
- (4) Medical history (PIPA Article 2, Paragraph 3);
- (5) Criminal record (PIPA Article 2, Paragraph 3);
- (6) Fact of having suffered damage by a crime (PIPA Article 2, Paragraph 3);
- (7) Fact of having physical disabilities, intellectual disabilities, mental disabilities (including developmental disabilities), or other physical and mental functional disabilities prescribed in the following (PIPA Enforcement Order Article 2; PIPA Enforcement Rules Article 5):
 - (i) physical disabilities set forth in an appended table of the Act for Welfare of Persons with Physical Disabilities (Act No.283 of 1949)
 - (ii) intellectual disabilities referred to under the Act for the Welfare of Persons with Intellectual Disabilities (Act No.37 of 1960)
 - (iii) mental disabilities referred to under the Act for the Mental Health and Welfare of the Persons with Mental Disabilities (Act No.123 of 1950) (including developmental disabilities prescribed in Article 2, Paragraph 2 of the Act on Support for Persons with Development Disabilities, and excluding intellectual disabilities under the Act for the Welfare of Persons with Intellectual Disabilities)
 - (iv) a disease with no cure methods established thereof or other peculiar diseases prescribed by cabinet order under Article 4, Paragraph 1 of the Act on Comprehensive Support for Daily and Social Lives of Persons with Disabilities (Act No. 123 of 2005), disability levels of which are equivalent to those prescribed by the Minister of Health, Labor and Welfare under the said Paragraph
- (8) Results of a medical check-up or other examination (hereinafter referred to as a “medical check- up

etc.”) for the prevention and early detection of a disease conducted on a principal by a medical doctor or other person engaged in duties related to medicine (hereinafter referred to as a “doctor etc.”) (PIPA Enforcement Order Article 2);

- (9) Fact that guidance for the improvement of the mental and physical conditions, or medical care or prescription has been given to a principal by a doctor etc. based on the results of a medical check-up etc. or for reason of disease, injury or other mental and physical changes (PIPA Enforcement Order Article 2);
- (10) Fact that an arrest, search, seizure, detention, institution of prosecution or other procedures related to a criminal case have been carried out against a principal as a suspect or defendant (PIPA Enforcement Order Article 2);
- (11) Fact that an investigation, measure for observation and protection, hearing and decision, protective measure or other procedures related to a juvenile protection case have been carried out against a principal as a juvenile or a person suspected thereof under Article 3, Paragraph 1 of the Juvenile Act (Act No.168 of 1948) (PIPA Enforcement Order Article 2).

Korea Addendum

(last updated 31 May 2022)

This addendum to the Personal Data Protection Policy applies to you if your Personal Data is being collected, used, disclosed or processed by us in Korea. The terms set out in this Korea Addendum are in addition to the terms set out in the Personal Data Protection Policy and form an integral part of the Personal Data Protection Policy. In the event of any conflict or inconsistency between the Personal Data Protection Policy and the terms of this Korea Addendum, this Korea Addendum shall govern and prevail.

1. Purposes for the Collection, Use and Disclosure of Your Personal Data

1.1 Without prejudice to the generality of the purposes notified to you in the Personal Data Protection Policy above, we may, in addition, also collect, use and disclose the items of your Personal Data specified below for the following specified purposes.

(a) if you are a job applicant:

General Personal Data/Personal Credit Information

| Classification | Purposes of Processing Personal Data | Items of Personal Data to be Processed |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Mandatory | <ul style="list-style-type: none"> HR management and job assignment: recruitment, processing your application, conducting background checks and due diligence, evaluating your application, making a hiring decision, assignment to departments, transfer to affiliates, etc. Compliance with law/performance of contracts: performance of any and all legal and administrative obligations imposed on GIC by the applicable laws and regulations, including compliance with labor laws including the Labor Standards Act and Industrial Safety and Health Act, compliance with internal regulations of GIC, and any obligations with regard to employee health and safety pursuant to the applicable laws and regulations, etc.; compliance with foreign workers related laws and regulations; performance of any and all legal and administrative obligations imposed on GIC by the applicable laws and regulations, including issuance and delivery of the receipt and tax invoices. | <ul style="list-style-type: none"> Name, gender, date of birth, age, address, home telephone number, mobile phone number, e-mail address, registered identification (ID), IP address, MAC address, nationality, photo, visual information, securities account number (including the name of account holder and financial institution), veteran & patriot information (registration number, classification, grade, relationship), other information specified in a bankbook such as bank account number, name of account holder and financial institution. Educational background (school name, location, major, year of entrance and year of graduation, graduation status, GPA, etc.), work experiences (company, title, responsible area, annual salary, details of salary payment, date of commencement of previous employment and date of retirement, service period, etc.), language skills (language, score/rank and date when such score/rank was achieved, and degree of fluency). Qualification/licenses (type, date of qualification/license, issuer), education/training (name of education/training program, certificate of completion), history of awards and/or disciplinary actions received (history of promotion, awards, disciplinary actions, performance evaluation records and details). |

| Classification | Purposes of Processing Personal Data | Items of Personal Data to be Processed |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | | <ul style="list-style-type: none"> • Matters related to military service (military branch, classification of military service, service period, occupational specialty). • Employment history, including dates of commencement of each employment period, responsible division, title, job descriptions, type of employment (including the date of change and contents thereof), details of salary payment(monthly base salary (gross and net), annual salary (gross and net), fixed bonuses, allowances, severance payment, retroactive salary, overtime data, etc.), work performance evaluation, etc. • Social insurance (status of subscription, insurance certificate number, date of acquisition, date of forfeiture, expiry date, status and period of reduction, beneficiary information, amount of benefit, etc.), group term life insurance. • Personal Data/Personal credit information of the job applicant or officer concerned and/or other third parties (name, department and job title, office address, e-mail address, telephone number, fax number, log-in records, etc. of third parties). • Professional Association Membership Details (e.g. Chartered Financial Analyst membership details). • Character referees. |
| Optional | <ul style="list-style-type: none"> • Evaluating your application, making a hiring decision. • Confirm whether you conduct your financial affairs properly so as to maintain financial soundness and to avoid financial embarrassment. • Obtain a declaration as to your financial soundness and monitor changes in such declaration. | <ul style="list-style-type: none"> • Personal data indicated under the mandatory collection and use. • History on prior refusals to applications for trade, business or professional license or restrictions thereto, prohibition or similar order in relation to financial services, dismissal or request to resign from office, employment or trust or fiduciary position, internal employment disciplinary proceedings or disqualifications from being a director or being engaged in any managerial capacity. |

| Classification | Purposes of Processing Personal Data | Items of Personal Data to be Processed |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | <ul style="list-style-type: none"> • Use as reference materials for personnel administration, work allocation, and salary management, etc. • Confirmation of persons subject to veterans' compensation and provision of appropriate treatment. • Communicating with you to inform you of changes and developments to GIC's policies, terms and conditions and other administrative information. • Sending you updates and alerts related to job applications which you may have requested for. • Conducting market research for statistical, profiling and statistical analysis for the improvement of services provided to you; managing the infrastructure and business operations of GIC and complying with internal policies and procedures, including providing you with access and/or use of websites, systems and infrastructure. • Conducting data analytics for the purpose of (i) system and process improvements, (ii) risk/fraud management, (iii) regulatory and compliance risk management, (iv) investment insights and (v) enhancements to human resources processes. • Dispute resolution, preventing, detecting and investigating non-compliance with laws, regulations, and internal corporate policies, including fraud and financial crimes, analysing and managing other commercial risks and risks arising from GIC's operations and investment activities. • Protecting and enforcing our contractual and legal rights and obligations. • Conducting audits, reviews and analysis of our internal processes. | <ul style="list-style-type: none"> • Personal financial standing, including matters related to unsatisfied judgment debts, bankruptcy petitions or compromise or scheme of arrangement with creditors. • Regulatory complaints, investigations, proceedings, warnings, convictions, sanctions, penalty, or matters relating to company or business in capacity as director or officer. • Financial affairs: whether job applicant is unable to repay any debt as it falls due, whether a statutory demand has been served on job applicant, whether there is any outstanding judgment debt against job applicant, etc. • Personal interests. • National merits, if any. |

Unique Identification Information

| Classification | Purposes of Processing Personal Data | Items of Personal Data to be Processed |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Mandatory | <ul style="list-style-type: none"> • Compliance with law/performance of contracts: performance of any and all legal and administrative obligations imposed on GIC by the applicable laws and regulations, including compliance with labor laws including the Labor Standards Act and Industrial Safety and Health Act, such as performance of employment agreement, compliance with internal regulations of GIC, and any obligations with regard to employee health and safety pursuant to the applicable laws and regulations, etc. issuance of a corporate card and fuel card. • HR management and job assignment: recruitment, processing your application, conducting background checks and due diligence, evaluating your application, assignment to departments, transfer to affiliates, etc. • Calculation of labor statistics data. | <ul style="list-style-type: none"> • Passport number, in the event the job applicant is a foreigner, his/her alien registration number. • Driver's license number (for positions that require a driver's license). • Unique Identification information (passport number, alien registration number, driver's license number) of the job applicant processed or monitored by the company through data processing and communications system, data processing devices including computers and smart phones, etc., data storage media, and e-mail accounts, etc. |

Sensitive Information

| Classification | Purposes of Processing Personal Data | Items of Personal Data to be Processed |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Mandatory | <ul style="list-style-type: none"> • Medical checkup. • Personnel administration. • Access, review, search, monitoring and retrieval of information assets including various electronic records, etc. and the status of processing thereof for the purpose of protection of fair profits of GIC such as protection of information processed in GIC and prevention of accidents, etc.; maintenance, upgrade and inspection of the security system; issuance of access card and maintenance and management of the access system; installation, management and operation of the visual information processing system for the prevention of crime, safety of facilities and prevention of fire, etc.; prevention of crime, violation of the company rules and other illegal acts, etc. that may arise in connection with work and procurement of evidence thereof, etc. | <ul style="list-style-type: none"> • Medical checkup results, medical certificates. • Physical and/or mental disability, types and level of disability, (if applicable) disabled registration number, registered matters of disability, information related to illness and injury (medical treatment information). • Health information, criminal records of the job applicant concerned. |
| Optional | <ul style="list-style-type: none"> • Facial verification for access to office premises • Realtime office security surveillance through the use of facial verification of Closed-Circuit Television (CCTV) feed to detect entry by unauthorized individuals | <ul style="list-style-type: none"> • Facial image data (including metadata) • Location data |

(b) if you are an employee, officer or owner of an external service provider or vendor

General Personal Data/Personal Credit Information

| Classification | Purposes of Processing Personal Data | Items of Personal Data to be Processed |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Mandatory | <ul style="list-style-type: none"> • Vendor management: processing applications, conducting background checks and due diligence, evaluating your application, managing the vendor relationship, including creating and maintaining the profiles of GIC's vendors and service providers in the systems databases etc. • Compliance with law/performance of contracts: performance of any and all legal and administrative obligations imposed on GIC by the applicable laws and regulations, including compliance with labor laws including the Labor Standards Act and Industrial Safety and Health Act, compliance with internal regulations of GIC; compliance with foreign workers related laws and regulations; performance of any and all legal and administrative obligations imposed on GIC by the applicable laws and regulations, including issuance and delivery of the receipt and tax invoices. • Handling of tax/insurance: subscription to, maintenance, procurement, and forfeiture of, and withdrawal from such insurance as may be required. | <ul style="list-style-type: none"> • Name, gender, date of birth, age, address, home telephone number, mobile phone number, e-mail address, registered identification (ID), nationality, photo, visual information. • Personal Data/ Personal credit information of the individual concerned (name, department and job title, office address, e-mail address, telephone number, fax number, log-in records, etc.). |
| Optional | <ul style="list-style-type: none"> • Confirm whether you conduct your financial affairs properly so as to maintain financial soundness and to avoid financial embarrassment. • Obtain a declaration as to your financial soundness and monitor changes in such declaration. • Use as reference materials for vendor administration and management. • Communicating with you to inform you of changes and developments to GIC's policies, terms and conditions and other administrative information. • Managing project tenders and quotations, processing orders or managing the supply of goods and services. • Creating and maintaining profiles of | <ul style="list-style-type: none"> • Personal data indicated under the mandatory collection and use. • Financial affairs: whether individual is unable to repay any debt as it falls due, whether a statutory demand has been served on individual, whether there is any outstanding judgment debt against individual, etc. |

| Classification | Purposes of Processing Personal Data | Items of Personal Data to be Processed |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------|
| | <p>our service providers and vendors in our system database.</p> <ul style="list-style-type: none"> • Processing and payment of vendor invoices and bills. • Conducting data analytics for the purpose of (i) system and process improvements, (ii) risk/fraud management, (iii) regulatory and compliance risk management, (iv) investment insights and (v) enhancements to human resources processes. • Dispute resolution, preventing, detecting and investigating non-compliance with laws, regulations, and internal corporate policies, including fraud and financial crimes, analysing and managing other commercial risks and risks arising from GIC's operations and investment activities. • Protecting and enforcing our contractual and legal rights and obligations. • Conducting audits, reviews and analysis of our internal processes. | |

Unique Identification Information

| Classification | Purposes of Processing Personal Data | Items of Personal Data to be Processed |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Mandatory | <ul style="list-style-type: none"> Handling of tax/insurance: subscription to, maintenance, procurement, and forfeiture of, and withdrawal from such insurance as may be required. Compliance with law/performance of contracts: performance of any and all legal and administrative obligations imposed on GIC by the applicable laws and regulations, including compliance with labor laws including the Labor Standards Act and Industrial Safety and Health Act, compliance with internal regulations of GIC; compliance with foreign workers related laws and regulations; performance of any and all legal and administrative obligations imposed on GIC by the applicable laws and regulations, including issuance and delivery of the receipt and tax invoices. | <ul style="list-style-type: none"> Passport number, resident registration numbers, in the event the individual is a foreigner, his/her alien registration number. Unique Identification information (passport number, alien registration number, driver's license number) of individual. |

Sensitive Information

| Classification | Purposes of Processing Personal Data | Items of Personal Data to be Processed |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| Mandatory | <ul style="list-style-type: none"> Facial verification for access to office premises Realtime office security surveillance through the use of facial verification of Closed-Circuit Television (CCTV) feed to detect entry by unauthorized individuals | <ul style="list-style-type: none"> Facial image data (including metadata) Location data |

1.2 In accordance with the Personal Information Protection Act (the "PIPA"), we may use or provide personal information within the scope reasonably related to the initial purpose of the collection, after duly considering whether disadvantages have been caused to data subjects and whether necessary security measures such as encryption etc. have been implemented. We will determine with due care whether to use or provide the personal information considering general circumstances, including relevant laws and regulations such as the PIPA, purpose of use or provision of the personal information, how the personal information will be used or provided, types of personal information to be used or provided, matters to which data subjects have provided consent or which were notified or informed to data subjects, impact on data subjects upon the use or provision of the personal information, and measures taken to protect the personal information. Specific considerations are as follows:

- Whether the additional use/provision is related to the initial purpose of the collection;

- Whether the additional use/provision is foreseeable in light of the circumstances under which personal information was collected and practices regarding processing;
- Whether the additional use/provision unfairly infringe on the interests of the data subject; and
- Whether the necessary security measures such as pseudonymization or encryption were taken.

2. Processing, Retention and Destruction of Personal Data

- 2.1 GIC will immediately destroy Personal Data when the purposes of processing such Personal Data are accomplished/ completed, in accordance with GIC's record retention policy and schedules, unless the applicable laws and regulations require GIC to preserve such Personal Data.

3. Procedures and Methods of Destroying Personal Data

- 3.1 GIC will select Personal Data for which the retention period has expired and then destroy such Personal Data in accordance with GIC's internal policies.
- 3.2 When GIC destroys Personal Data, it will implement measures to ensure, to the best of its ability, that the information is not restored or regenerated.
- 3.3 If GIC has to retain Personal Data instead of destroying it, GIC will store and manage such Personal Data or such Personal Data file separately from other Personal Data.
- 3.4 If the Personal Data that needs to be destroyed is in the form of electronic file, GIC will delete such information and such information will not be restored or regenerated unless required by applicable law or regulation. Any other document, printout, letter and other recorded media will be destroyed by incinerating or shredding them into pieces.

4. Disclosure of Personal Data

- 4.1 Without prejudice to the general list of third parties to whom your Personal Data may be disclosed as set out in this Personal Data Protection Policy, GIC may, in addition, transfer your Personal Data to the following third parties as summarised below.

(a) if you are job applicant:

General Personal Data - Mandatory

| Recipient Name | Country where Recipient is Located | Recipient's Purpose of Using the Personal Data | Items of Personal Data to be Transferred | Period of Retention and Use by Recipient |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|------------------------------------------------------------|
| GIC PRIVATE LIMITED and affiliates (including GIC REAL ESTATE PRIVATE LIMITED, GIC SPECIAL INVESTMENTS PRIVATE LIMITED, and GIC ASSET MANAGEMENT PRIVATE LIMITED)* | Various* | <ul style="list-style-type: none"> • To fulfill administrative/ regulatory requirements • Personnel management | All items of general Personal Data / personal credit information collected by GIC as above | Until the purposes of using the Personal Data are attained |

Unique Identification Information - Mandatory

| Recipient Name | Country where Recipient is Located | Recipient's Purpose of Using the Unique Identification Information | Items of Unique Identification Information to be Transferred | Period of Retention and Use by Recipient |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| GIC PRIVATE LIMITED and affiliates (including GIC REAL ESTATE PRIVATE LIMITED, GIC SPECIAL INVESTMENTS PRIVATE LIMITED, and GIC ASSET MANAGEMENT PRIVATE LIMITED)* | Various* | <ul style="list-style-type: none"> To fulfil administrative/regulatory requirements Personnel management | All items of unique identification information collected by GIC as above | Until the purposes of using the unique identification information are attained |

Sensitive Information - Mandatory

| Recipient Name | Country where Recipient is Located | Recipient's Purpose of Using the Sensitive Information | Items of Sensitive Information to be Transferred | Period of Retention and Use by Recipient |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|--------------------------------------------------------------------|
| GIC PRIVATE LIMITED and affiliates (including GIC REAL ESTATE PRIVATE LIMITED, GIC SPECIAL INVESTMENTS PRIVATE LIMITED, and GIC ASSET MANAGEMENT PRIVATE LIMITED)* | Various* | <ul style="list-style-type: none"> To fulfil administrative/regulatory requirements Personnel management | All items of sensitive information collected by GIC as above | Until the purposes of using the sensitive information are attained |

* GIC has been transferring personal information including unique identification information and sensitive information to third party recipients including GIC headquarters/affiliates. Please see <http://www.gic.com.sg/contact> for information on the GIC headquarters/affiliates.

5. Delegation of Personal Data Processing Services

- 5.1 GIC delegates Personal Data processing services as follows and will notify any changes in the delegates and the details of delegated services through this Korea Addendum.

| Delegatee | Details of Delegated Services |
|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| GIC PRIVATE LIMITED | Reviewing and processing the job applicant's application; reviewing the vendor's profile and managing the vendor relationship; operating and managing office security systems (including facial verification systems) and providing technical support |
| GIC REAL ESTATE PRIVATE LIMITED | Reviewing and processing the job applicant's application; reviewing the vendor's profile and managing the vendor relationship |
| GIC SPECIAL INVESTMENTS PRIVATE LIMITED | Reviewing and processing the job applicant's application; reviewing the vendor's profile and managing the vendor relationship |
| GIC ASSET MANAGEMENT PRIVATE LIMITED | Reviewing and processing the job applicant's application; reviewing the vendor's profile and managing the vendor relationship |
| SAP ASIA PTE LTD | Operating and managing the server that stores the Personal Data collected by GIC and providing technical support to GIC |
| Symphony Communication Services, LLC | Operating and managing the server that stores the Personal Data collected by GIC and providing technical support to GIC |
| Microsoft Operations Pte Ltd | Operating and managing the servers that store the Personal Data collected by GIC and providing technical support to GIC |
| Sinovision Technology Private Limited | Operating and managing office security systems (including facial verification systems) and providing technical support |
| Yitu Private Limited | Operating and managing the office security system (including facial verification systems) and providing technical support |

6. Protection of Personal Data

- 6.1 The security of your Personal Data is important to us. In accordance with privacy laws, we have adopted reasonable security practices and procedures to safeguard the Personal Data under our control against unauthorised access, disclosures and other similar risks. Access to your Personal Data is restricted to those parties who need to know such Personal Data in relation to the purposes specified in this Personal Data Protection Policy.
- 6.2 While we will endeavour to take all reasonable and appropriate steps to keep secure any Personal Data under our control, you acknowledge and agree that we cannot provide any absolute guarantees regarding the security of your Personal Data.

7. Deletion of Personal Data; Suspension of Processing of Personal Data

- 7.1 In addition to the rights granted under the main Personal Data Protection Policy, if you would like to request the deletion of your Personal Data or the suspension of the processing of your Personal Data or would like to contact us with complaints or to seek relief regarding your Personal Data (subject to our rights at law), please contact GIC as follows:

Department: Legal and Compliance

Email: GrpLCD_PersonalData@gic.com.sg

Number: +65 6889 8888

- 7.2 In any of the following cases, GIC may refuse the request for suspension of processing of

Job applicants, vendors, members of the public and investment counterparties

Personal Data made by an individual:

- (a) if there is a special provision in law or if denying the request is necessary to comply with legal obligations;
- (b) if such an act is likely to inflict damages upon another person's life or body or unfairly infringe upon another person's property and other rights; or
- (c) if performing the contract becomes difficult (i.e. unable to provide the agreed services) unless the Personal Data is processed, and the individuals have not expressed a clear intention to terminate such contract.

UK Addendum

(last updated 15 February 2023)

This addendum to the Personal Data Protection Policy applies to you if your Personal Data is being collected, used, disclosed or processed by us in the UK. The information set out in this UK Addendum relates solely to UK related processing of Personal Data, and in the event of any conflict or inconsistency between the Personal Data Protection Policy and the terms of this UK Addendum, this UK Addendum shall govern and prevail.

This UK Addendum sets out the basis on which any of your Personal Data will be collected, stored and used by us.

QUICK GUIDE TO CONTENTS

1. [Introduction](#)
2. [What Personal Data does GIC collect?](#)
3. [How does GIC use Personal Data?](#)
4. [Does GIC disclose Personal Data?](#)
5. [How long does GIC retain Personal Data?](#)
6. [How does GIC transfer Personal Data?](#)
7. [How does GIC keep Personal Data secure?](#)
8. [Your Privacy Rights](#)
9. [Changes to this UK Addendum](#)
10. [Contact Us](#)

9. Introduction

- 9.1 For the purposes of the General Data Protection Regulation, the data controllers of your Personal Data will be the entity you interact (or intend to interact) with. If within the United Kingdom this will be either GIC Private Limited, GIC (London) Private Limited or GIC Real Estate International Pte Ltd, London Office (collectively termed as “GIC” in this UK Addendum). If your application relates to any of our other entities outside the United Kingdom, please see the relevant countries’ Addendum(s) for information on how your Personal Data is processed. GIC Private Limited (where GIC’s Head Office is located), may also be a joint data controller of your Personal Data in certain circumstances.

10. What Personal Data does GIC collect?

- 10.1 We collect and process your Personal Data in the following ways:

Personal Data you give us directly

- (a) when you submit forms or applications to us;
- (b) when you submit your resumes and/or CVs to us;
- (c) when you submit queries, requests, complaints or feedback to us;
- (d) when you respond to our request for additional Personal Data;
- (e) when you ask to be included in an email or other mailing list;

- (f) when you respond to our initiatives or contact us;
- (g) when you take part in events organised by GIC;
- (h) when you give your business card to any of our employees or representatives;
- (i) when you visit any of our offices and provide visitor information;
- (j) when you are captured by any of the CCTV cameras on our premises;
- (k) when you are employed or engaged by GIC;
- (l) when you register to be a part of our alumni network; and
- (m) when you submit your Personal Data to us for any other reasons.

Personal Data we collect from third parties

- (a) when you are an employee of an organisation or counterparty we do business with or otherwise engaged by such organisation or counterparty to do work that involves GIC;
- (b) when counterparties or introducers refers you to us as a potential organisation or counterparty to do business with or engaged to do work that involves GIC;
- (c) when you enter into an agreement involving any GIC owned asset with any of our managers or other representatives; and
- (d) when you take part in events organised by GIC jointly with any other third party or events organised solely by a third party; and
- (e) when a recruitment agency refers your resume to us;

Personal Data we collect automatically

We collect certain information by automated means, such as cookies and web beacons, whenever you browse our website. This could include IP address, browser type, operating system, referring URLs, information on actions taken on our websites, and dates and times of visits.

Personal Data you provide about another person

In certain circumstances, you provide us with Personal Data of other people (e.g. information of your dependents, spouse, children and/or parents). By submitting such information to us, you represent and warrant to us that they have read and understood this Personal Data Protection Policy and that you have obtained the requisite consent of such third party and/or are authorized to provide us with such Personal Data for the relevant purposes contained in this Addendum.

- 10.2 You are to ensure that all Personal Data submitted to us is complete, accurate, true and correct. Failure on your part to do so or where you decline to provide certain Personal Data we require, may result in our inability to provide you with the relevant services/ support. This is also the case where we require certain Personal Data and you decline to provide this.

11. How does GIC use Personal Data?

11.1 We generally collect, use, disclose and process your Personal Data and Personal Data of others you pass to us for the following purposes:

(a) To provide a requested service or carry out a contract with you

- (i) carrying out our obligations arising from any contract we enter into with you.

(b) Where we have your consent

- (i) contacting you, including by email, SMS and telephone to provide you with direct marketing communications, including newsletters and event invites. We will only do so when we receive your consent and in line with your preferences on the communications that you have indicated. You may opt-out or retract your consent to receive such communications at any time;
- (ii) photographs and/or video recordings may be taken at events which you have attended and used and disclosed for our marketing and/or promotional purposes. Such photographs and videos may be published on our website, social media channels or made publicly available to recipients overseas for our marketing and/or promotional purposes.

(c) Where we have a legitimate interest

- (i) contacting you, including by email, SMS, messaging services such as Whatsapp, WeChat, etc and telephone in the ordinary course of our investment and operational activities, where we have a business relationship with you. You are able to object to receiving such communications at any time;
- (ii) investigating and addressing enquiries, questions and complaints and responding to any feedback;
- (iii) managing the infrastructure and business operations of GIC and complying with internal policies and procedures, including providing you with access and/or use of websites, systems and infrastructure;
- (iv) facilitating investments, business asset transactions (which may include but is not limited to any merger, acquisition or asset sale) and business agreements with counterparties;
- (v) matching any Personal Data we hold which relates to you for any of the purposes listed herein;
- (vi) verifying your identity and conducting background checks and due diligence;
- (vii) conducting profiling and data analytics for the purpose of (i) system and process improvements, (ii) risk/fraud management, (iii) regulatory and compliance risk management, (iv) investment insights and (v) enhancements to human resources processes;
- (viii) dispute resolution, preventing, detecting and investigating non-compliance with laws, regulations, and internal corporate policies, including fraud and financial crimes, analysing and managing other commercial risks and risks arising from GIC's operations and investment activities;
- (ix) protecting and enforcing our contractual and legal rights and obligations;
- (x) conducting audits, reviews and analysis of our internal processes; and/or
- (xi) fulfilling GIC's legal, contractual or regulatory obligations, including complying with any applicable laws, regulations, rules, codes of practice or guidelines or to assist in law enforcement and investigations by relevant authorities;

- if you are an employee, officer or owner of an external service provider or vendor:
 - (i) verifying and processing your personal particulars and assessing your organisation's and/or your suitability, eligibility or qualification as an external service provider or vendor for GIC as well as your organisation's and your financial status;
 - (ii) communicating with you to inform you of changes and developments to GIC's policies, terms and conditions and other administrative information;
 - (iii) managing project tenders and quotations, processing orders or managing the supply of goods and services;
 - (iv) creating and maintaining profiles of our service providers and vendors in our system database;
 - (v) processing and payment of vendor invoices and bills; and/or;
 - (vi) purposes reasonably related to any of the above.
- if you are an employee, officer or owner of our investment counterparties, including our joint venture partners, brokers, investee companies etc
 - (i) verifying and processing your personal particulars to maintain accurate records;
 - (ii) communicating with you to inform you of changes and developments to GIC's policies, terms and conditions and other administrative information;
 - (iii) creating and maintaining profiles of our investment counterparties in our system database; and/or
 - (iv) purposes reasonably related to any of the above.
- if you are a job applicant:
 - (i) verifying and processing your personal particulars, processing your application, evaluating your suitability, eligibility or qualification for employment with GIC as well as assessing your financial status;
 - (ii) communicating with you to inform you of changes and developments to GIC's policies, terms and conditions and other administrative information;
 - (iii) sending you updates and alerts related to job applications which you may have requested for;
 - (iv) conducting market research for statistical, profiling and statistical analysis for the improvement of services provided to you; and/or
 - (v) purposes reasonably related to any of the above.

11.2 Where we rely on legitimate interest as a grounds for processing, we carry out a 'balancing test' to ensure that our processing is necessary and that your fundamental rights of privacy are not outweighed by our legitimate interests, before we go ahead with such processing. We keep a record of these balancing tests. **You have a right to the information contained in these balancing tests on request, and can find out more by contacting us via the details in Section 10.**

- 11.3 In many cases, you will be obliged to provide your Personal Data to us, because we will need it (for example to manage our relationship with you). However, there may be some instances where the provision of your Personal Data is voluntary. We will notify you of this at the point of data collection.
- 11.4 In the event that we collect any Special Category of Personal Data about you during our employee recruitment process which relates to criminal offences information for the purposes of carrying out background checks, we collect only personal data necessary for these background checks and will only do this where you have been informed and have given your explicit consent to our collection and use of your Special Category of Personal Data.

12. Does GIC disclose Personal Data?

- 12.1 GIC will take reasonable steps to protect your Personal Data against unauthorised disclosure. Subject to the provisions of any applicable law, your Personal Data may be disclosed to the parties listed below (whether located in your local jurisdiction or overseas), for the purposes listed above (where applicable) to:
- (a) other entities within the GIC group for internal reasons, primarily for business and operational purposes in line with this policy;
 - (b) insurance companies and brokers in connection with staff insurance;
 - (c) recruitment agencies;
 - (d) agents, contractors or third party service providers who provide operational services to GIC, such as courier services, telecommunications, information technology, advertising, payment, payroll, processing, training, employment, market research, storage, archival, customer support, investigation services or other services to GIC;
 - (e) any business partner, investor, assignee or transferee (actual or prospective) to facilitate business asset transactions (which may extend to any mergers, acquisitions and debt or asset sale);
 - (f) banks, regulators advisers and deal counterparties where necessary for the purposes of carrying out KYC checks;
 - (g) local and overseas financial institutions and their respective service providers;
 - (h) our professional advisers such as our consultants, auditors and lawyers;
 - (i) business and charity partners in relation to events planning;
 - (j) with trusted third-party suppliers of information verification services where necessary for the purposes of validating the information you provide to us in the course of interacting with us or entering into a contract with us;
 - (k) relevant government regulators, government ministries, statutory boards, embassies, or authorities and/or law enforcement agencies, whether local or overseas, to comply with any directions, laws, regulations, rules, codes of practice or guidelines, or schemes issued or administered by any of them;
 - (l) marketing and social media partners in relation to marketing and/or promotional photographs and videos published on our website, social media channels or otherwise made publicly available to recipients overseas; and/or
 - (m) any other party to whom you authorise us to disclose your Personal Data.

13. How long does GIC retain Personal Data?

- 13.1 We only retain your Personal Data for as long as is necessary for us to use your information for the purposes outlined in this UK Addendum. Please be advised that we may retain some of your information after you cease to interact with GIC, for instance if this is necessary in the interest of our legitimate interest such as for business administration purposes.
- 13.2 We retain your Personal Data in accordance with our internal Record Retention Policy. When determining the relevant retention periods, the following factors may form part of the overall consideration:
- (a) our contractual obligations and rights in relation to the Personal Data involved;
 - (b) legal obligation(s) under applicable law to retain data for a certain period;
 - (c) our legitimate interest where we have carried out a balancing test;
 - (d) statute of limitations under applicable law(s);
 - (e) (potential) disputes/litigation; and / or
 - (f) guidelines issued by relevant data protection authorities.

Otherwise, we securely erase your information where we no longer require your Personal Data for the purposes collected and have no legitimate reason to retain such Personal Data.

14. How does GIC transfer Personal Data?

Your Personal Data will be stored in external servers located in Australia, Singapore, Hong Kong, Germany and Netherlands. We may also transfer your Personal Data for the purposes stated in this UK Addendum, to parties located in other countries and territories outside the UK or outside the EEA (e.g. to the GIC head office in Singapore). We will endeavour to inform you of the countries that your Personal Data will be transferred to prior to any such transfers. You may also reach out to us via the contact details in Section 10 "Contact Us" at any point of time to have the latest list of countries.

Where your Personal Data is transferred to locations outside the EEA, we ensure adequate measures are in place to offer equivalent protection as your information would receive within the EEA and in compliance with the EU General Data Protection Regulation 2016/679. We have in place EU Model Contractual Clauses as an adequate safeguard for transfers outside the EEA and between GIC entities which are governed by our intra-group transfer agreement. To find out more about how we safeguard your information in relation to transfers outside the EEA, please contact us via the contact details in Section 10 "Contact Us".

15. How does GIC keep Personal Data secure?

- 15.1 We maintain appropriate administrative, technical and physical safeguards to protect your personal data against loss, misuse, unauthorised access, disclosure, alteration or destruction.

16. **Your Privacy Rights**

By law, you have a number of rights (subject to certain conditions) when it comes to your Personal Data. Further information and advice about your rights can be obtained from the data protection regulator in your country. You can exercise any of these rights by contacting us via the details in Section 10 below:

| Rights | What does this mean? |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| The right to object to processing | You have the right to object to certain types of processing, including the purpose of contacting you, including by email, SMS, messaging services such as What Sapp, WeChat, etc and telephone in the ordinary course of our investment and operational activities, where we have a business relationship with you. |
| The right to be informed | You have the right to be provided with clear, transparent and easily understandable information about how we use your Personal Data and your rights. This is why we're providing you with the information in this Addendum. If we intend to use your Personal Data in a way not covered by this policy, we will continue to keep you informed prior to any such use. |
| The right of access | You have the right to obtain access to your Personal Data (if we're processing it), and certain other information (similar to that provided in this Addendum). This is so that you are aware and can check that we are using your Personal Data in accordance with data protection law. |
| The right to rectification | You are entitled to have your Personal Data corrected if it is inaccurate or incomplete. |
| The right to erasure | This is also known as 'the right to be forgotten' and, in simple terms, enables you to request the deletion or removal of your Personal Data where there is no compelling reason for us to keep using it. This is not a general right to erasure though there are exceptions. |
| The right to restrict processing | You have rights to 'block' or suppress further use of your Personal Data. When processing is restricted, we can still store your Personal Data, but may not use it further. We keep lists of people who have asked for further use of their Personal Data to be 'blocked' to make sure the restriction is respected in future. |
| The right to data portability | You have rights to obtain and reuse your information for your own purposes across different services. For example, if you decide to switch to a new provider, this enables you to move, copy or transfer your information easily between our IT systems and theirs safely and securely, without affecting its usability. |
| The right to lodge a complaint | You have the right to lodge a complaint about the way we handle or process your information with your relevant national data protection regulator. See details of the UK data protection regulator via the details in Section 10. |
| The right to withdraw consent | If you have given your consent to anything we do with your Personal Data, you have the right to withdraw your consent at any time (although if you do so, it does not mean that anything we have done with your consent up to that point is unlawful). This includes the right to withdraw consent to us using your Personal Data for marketing purposes. |

- 16.1 We usually act on the requests to exercise these rights and provide information free of charge, but may charge a reasonable fee to cover our administration costs of providing the information for baseless or excessive/repeated requests or further copies of the same information. Alternatively, we may be entitled to refuse to act on the request.

Please consider your request responsibly before submitting it. We will respond to any requests as soon as we can. Generally, this will be within one month from when we receive your request but, if the request is going to take longer to deal with, we will let you know in advance.

17. Changes to this UK Addendum

- 17.1 We may periodically make changes to this UK Addendum. We will endeavour to notify you of any significant changes where we have a relationship with you and otherwise post updated versions on this page. We recommend that you revisit this page regularly for any updates.

18. Contact Us

- 18.1 If you:

- (a) have any questions or feedback relating to your Personal Data or our Personal Data Protection Policy (in particular this Addendum); or
- (b) would like to obtain information about or exercise any of your Rights as set out in this Personal Data Protection Policy, contact:

Name: Lynn Hew Ooi Lyn

Email: lynnhew@gic.com.sg

Contact number: +65-68898377

If you are not satisfied with our response to a complaint you have made, or think we are not complying with data protection law, you can make a complaint to the UK data protection regulator - the Information Commissioner's Office:

Address: Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

Phone number: 0303 123 1113

Website: <https://ico.org.uk/make-a-complaint/>

US Addendum

(last updated 15 February 2023)

This addendum to the Personal Data Protection Policy applies to you if your Personal Data is being collected, used, disclosed or processed by us in the United States. The terms set out in this US Addendum are in addition to the terms set out in the Personal Data Protection Policy and form an integral part of the Personal Data Protection Policy. In the event of any conflict or inconsistency between the Personal Data Protection Policy and the terms of this US Addendum, this US Addendum shall govern and prevail.

GIC Private Limited and its subsidiaries, its overseas offices and relevant investment holding / management services companies, as well as its representatives and/or agents (collectively referred to herein as “GIC”) adopts this Addendum to comply with the California Consumer Privacy Act of 2018 (“CCPA”) and any terms defined in the CCPA have the same meaning when used in this Addendum. If you are a GIC employee, please refer to the GIC Employee Personal Data Protection Policy.

1. **Information We Collect**

1.1 We collect information from California residents that identifies, relates to, describes, references, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or device (“**personal information**”). In particular, GIC has collected the following categories of personal information within the last twelve (12) months:

| Category | Examples ¹ | Sources | Purpose | Disclosures for a Commercial or Business Purpose |
|--------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A. Identifiers | A real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, Social Security number, driver's license number, passport number, or other similar identifiers. | a) Directly or indirectly from you b) From third parties | a) Providing and operating our website and other services b) Business and human resource management and operations c) Compliance with law or performance of contracts d) Maintenance of safety and security of facilities and assets e) Job assignment f) Career management g) Payment of salaries h) Welfare i) Handling of tax/insurance | a) Service providers b) Insurance providers c) Payroll service providers d) Government regulators or entities e) Parties to a corporate transaction or proceeding |
| B. Personal information categories listed in the | A name, signature, Social Security number, physical characteristics or | a) Directly or indirectly from you b) From third | a) Providing and operating our website and other services | a) Service providers b) Insurance providers |

¹ Examples listed herein are illustrative of the types of personal information included in each category and may or may not be the specific types of personal information collected on an individual. Additionally, some personal information included in these categories may overlap with other categories.

| Category | Examples ¹ | Sources | Purpose | Disclosures for a Commercial or Business Purpose |
|-----------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| California Customer Records statute (Cal. Civ. Code § 1798.80(e)) | description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information. | parties | <ul style="list-style-type: none"> b) Business and human resource management and operations c) Compliance with law or performance of contracts d) Maintenance of safety and security of facilities and assets e) Job assignment f) Career management g) Payment of salaries h) Welfare i) Handling of tax/insurance | <ul style="list-style-type: none"> c) Payroll service providers d) Government regulators or entities e) Parties to a corporate transaction or proceeding |
| C. Protected classification characteristics under California or federal law | Race, ancestry, physical disability, mental disability, medical condition, genetic information, marital status, sex (which includes pregnancy, childbirth, breastfeeding, and related medical conditions), gender, gender identity, gender expression, age, sexual orientation, military or veteran status, immigration/ citizenship status or related protected activities, protected medical leaves, or any other category or activity protected by federal, state, or local laws, ordinances, or regulations. | a) Directly from you | <ul style="list-style-type: none"> a) Providing and operating our website and other services b) Business and human resource management and operations c) Compliance with law or performance of contracts d) Fraud prevention e) Maintenance of safety and security of facilities and assets f) Reports of employment figures to government agencies regulators g) Workers' Compensation insurance requirements h) Personnel administration and improvement of working environment | <ul style="list-style-type: none"> a) Service providers b) Insurance providers c) Government regulators or entities d) Parties to a corporate transaction or proceeding |
| D. Biometric information | Genetic, physiological, | a) Directly or indirectly | a) Complying with internal | <ul style="list-style-type: none"> a) Service providers b) Insurance providers |

| Category | Examples ¹ | Sources | Purpose | Disclosures for a Commercial or Business Purpose |
|--------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| | behavioural, and biological characteristics, or activity patterns used to extract a template or other identifier or identifying information, such as, fingerprints, faceprints, and voiceprints, iris or retina scans, keystroke, gait, or other physical patterns, and sleep, health, or exercise data. | from you b) From third parties | policies and procedures b) Providing access/use of systems or infrastructure c) Maintenance of safety and security of facilities and assets | c) Government regulators or entities d) Parties to a corporate transaction or proceeding |
| E. Internet or other similar network activity. | Browsing history, search history, information on a consumer's interaction with a website, application, or advertisement. | (a) Directly or indirectly from you (b) From third parties | a) Fraud prevention b) Maintenance of safety and security of facilities and assets | a) Analytics and business intelligence vendors b) Cybersecurity vendors c) Service providers d) Government regulators or entities |
| G. Professional or employment-related information | Current or past job history. | a) Directly from you b) From third parties | a) Human resource management and job assignment b) Career management | a) Service providers b) Insurance providers c) Government regulators or entities d) Parties to a corporate transaction or proceeding |
| H. Non-public education information (per the Family Educational Rights and Privacy Act (20 U.S.C. Section 1232g, 34 C.F.R. Part 99)) | Education records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades, transcripts, class lists, student schedules, student identification codes, student financial information, or student disciplinary records. | a) Directly from you | a) Human resource management and job assignment b) Career management | a) Service providers b) Insurance providers c) Government regulators or entities d) Parties to a corporate transaction or proceeding |

SENSITIVE PERSONAL INFORMATION

| Category | Examples ² | Sources | Purpose | Disclosures for a Commercial or Business Purpose |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Government ID | Government-issued identifiers such as driver's license, passport number, and social security numbers | a) Directly or indirectly from you b) From third parties | a) Providing and operating our website and other services b) Business and human resource management and operations c) Compliance with law or performance of contracts d) Maintenance of safety and security of facilities and assets e) Job assignment f) Career management g) Payment of salaries h) Welfare i) Handling of tax/insurance | a) Service providers b) Insurance providers c) Payroll service providers d) Government regulators or entities e) Parties to a corporate transaction or proceeding |
| Account access information | Information such as a username or account number in combination with a password, security or access code, or other credential that allows access to an account | Directly or indirectly from you | a) Providing and operating our website and other services b) Business and human resource management and operations c) Compliance with law or performance of contracts d) Maintenance of safety and security of facilities and assets e) Job assignment f) Career management g) Payment of salaries h) Welfare i) Handling of tax/insurance | a) Service providers b) Insurance providers c) Payroll service providers d) Government regulators or entities e) Parties to a corporate transaction or proceeding |

² Examples listed herein are illustrative of the types of personal information included in each category and may or may not be the specific types of personal information collected on an individual employee or job applicant. Additionally, some personal information included in these categories may overlap with other categories.

| Category | Examples ² | Sources | Purpose | Disclosures for a Commercial or Business Purpose |
|----------------------------|----------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Sensitive demographic data | Information about racial or ethnic origin, religious or philosophical beliefs, or union membership | Directly from you | <ul style="list-style-type: none"> a) Providing and operating our website and other services b) Business and human resource management and operations c) Compliance with law or performance of contracts d) Reports of employment figures to government agencies regulators e) Workers' Compensation insurance requirements f) Personnel administration and improvement of working environment | <ul style="list-style-type: none"> a) Service providers b) Insurance providers c) Government regulators or entities |
| Contents of communications | Contents of mail, email, and text messages | <p>Directly or indirectly from you</p> <p>[For vendors with access to GIC system access, presumably GIC already has access to this data?]</p> | <ul style="list-style-type: none"> a) Providing and operating our website and other services b) Business and human resource management and operations c) Compliance with law or performance of contracts d) Fraud prevention e) Maintenance of safety and security of facilities and assets f) Personnel administration and improvement of working environment g) Complying with internal policies and procedures h) Providing access/use of systems or infrastructure | <ul style="list-style-type: none"> a) Analytics and business intelligence vendors b) Cybersecurity vendors c) Service providers d) Government regulators or entities |
| Biometric information | Biometric information used for the | a) Directly or indirectly from you | a) Complying with internal policies and procedures | <ul style="list-style-type: none"> a) Service providers b) Insurance providers |

| Category | Examples ² | Sources | Purpose | Disclosures for a Commercial or Business Purpose |
|-------------|------------------------------------------|-------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| | purpose of uniquely identifying a person | b) From third parties | b) Providing access/use of systems or infrastructure c) Maintenance of safety and security of facilities and assets | c) Government regulators or entities |
| Health data | Information concerning a person's health | a) Directly or indirectly from you b) From third parties | a) Providing and operating our website and other services b) Business and human resource management and operations c) Compliance with law or performance of contracts d) Fraud prevention e) Maintenance of safety and security of facilities and assets f) Reports of employment figures to government agencies regulators g) Workers' Compensation insurance requirements h) Personnel administration and improvement of working environment | a) Service providers b) Insurance providers c) Government regulators or entities |

1.2 Personal information does not include:

- (a) Publicly available information from government records.
- (b) Deidentified or aggregated consumer information.
- (c) Information excluded from the CCPA's scope, like:
 - (i) health or medical information covered by the Health Insurance Portability and Accountability Act of 1996 ("**HIPAA**") and the California Confidentiality of Medical Information Act ("**CMIA**") or clinical trial data;
 - (ii) personal information covered by certain sector-specific privacy laws, including the Fair Credit Reporting Act ("**FCRA**"), the Gramm-Leach-Bliley Act (GLBA) or

Job applicants, vendors, members of the public and investment counterparties

California Financial Information Privacy Act (“**FIPA**”), and the Driver’s Privacy Protection Act of 1994.

- 1.3 GIC obtains the categories of personal information listed above from the following categories of sources:
- (a) Directly from you. For example, from forms or applications you complete.
 - (b) Indirectly from you. For example, from observing your interactions with company systems or our products or services.
 - (c) Third Parties. For example, from vendors used for job applicant background checks.

2. Use of Personal Information

- 2.1 We may use or disclose the personal information. For information related to the way GIC uses your personal information, please refer to section 3.1 of the Personal Data Protection Policy above.
- 2.2 GIC will not collect additional categories of personal information or use the personal information we collected for materially different, unrelated, or incompatible purposes without providing you notice.

3. Retention of Personal Information

- 3.1 We retain personal information for as long as necessary to provide our website and services, operate our business, fulfil transactions, comply with our legal obligations, resolve disputes, enforce our agreements, and other legitimate and lawful business purposes.

4. California Consumer Privacy Rights

If you are a California resident, you have certain privacy rights under the California Consumer Privacy Act (“**CCPA Rights**”). This section describes those rights and how you can exercise them with GIC.

4.1 CCPA Rights Requests

(a) Right to Know

You can request information on the personal information we have collected about you in the preceding 12 months, including:

- (i) the specific pieces of personal information we have collected about you.
- (ii) the following categories of information:
 - categories of personal information we have collected about you.
 - categories of sources from which the personal information was collected.
 - our business or commercial purpose for collecting or selling the personal information.
 - the categories of third parties with whom we shared personal information.

To submit a request to know, please send an email to GrpLCD_PersonalData@gic.com.sg. You must use “California Request to Know Information” or “California Right to Know Categories” in the subject line of your email, as appropriate. You must provide us with your first name, last name, email address, and phone number. To verify your identity, we will match that information to the information we have on our systems. To designate an authorized agent to act on your behalf you must send a signed, written authorization containing your first name, last name, email address, and phone number to GrpLCD_PersonalData@gic.com.sg.

You must provide us with all of the information set forth above in any such request, including what request you are making.

(b) Right to Correction

You can request that we correct any inaccurate personal information we may have about

you. We may deny your request if we determine that the personal information is likely accurate, the request is fraudulent, or as otherwise permitted by law. We will also maintain a record of your CCPA Rights requests.

To submit a correction request, please send an email to GrpLCD_PersonalData@gic.com.sg. You must use "California Request to Correct" in the subject line of your email. You must provide us with your [first name, last name, email address, and phone number] as well as any documentation demonstrating that the personal information is inaccurate. To verify your identity, we will match that information to information we have on our systems. To designate an authorized agent to act on your behalf you must send a signed, written authorization containing your first name, last name, email address, and phone number to GrpLCD_PersonalData@gic.com.sg.

You must provide us with all of the information set forth above in any such request.

(c) **Right to Deletion**

- (i) You can also request that we delete your personal information. We may not delete all of your personal information if one of the following exceptions applies:
 - Transactional: to complete a transaction for which the personal information was collected, provide a good or service requested by you, or perform a contract we have with you;
 - Security: to detect and prevent data security incidents;
 - Error Correction: to debug or repair any errors;
 - Legal: to protect against fraud or illegal activity or to comply with applicable law or a legal obligation, or exercise rights under the law, such as the right to free speech; or
 - Internal Use: to use your personal information, internally, in a lawful manner that is compatible with the context in which you provided the information (i.e. to improve our services).
- (ii) We will also maintain a record of your CCPA Rights requests.
- (iii) Please note that if we delete your personal information, some of our services will not work the same. For example, your previous opt out requests will not be saved and saved preferences and information will no longer be available.

To submit a request to delete, please send an email to GrpLCD_PersonalData@gic.com.sg. You must use "California Request to Delete" in the subject line of your email. You must provide us with your [first name, last name, email address, and phone number]. To verify your identity, we will match that information to the information we have on our systems. To designate an authorized agent to act on your behalf you must send a signed, written authorization containing your first name, last name, email address, and phone number to GrpLCD_PersonalData@gic.com.sg.

You must provide us with all of the information set forth above in any such request.

4.2 **Do Not Sell or Share My Personal Information; Right to Opt-Out**

California residents have the right to opt out of the "sale" or "sharing" of your personal information to third parties, as those terms are defined in the CCPA.

GIC does not presently exchange personal information for money with anyone, nor does GIC otherwise disclose personal information within the meaning of "sale" or "share" as defined by the CCPA. However, if you would like to opt out of the "sale" or "sharing" of your personal information as permitted under CCPA in the event we do "sell" or "share" personal information in the future, you can do so and we will keep a record of this request.

To submit a request to opt out of the "sale" or "sharing" of your personal information, please email us at GrpLCD_PersonalData@gic.com.sg. You must use "California Opt Out from Sale or Sharing" in the subject line of your email and provide us with your full name and email address.

In order to designate an authorized agent to act on your behalf, you must send a signed, written authorization containing your first name, last name, email address, and phone number to GrpLCD_PersonalData@gic.com.sg.

You can also write to us at the address above to submit your request by mail. Please include a heading or subject line "California Opt Out from Sale or Sharing" in your letter and provide us with your full name and email address.

4.3 **Right to Limit Use and Disclosure of Sensitive Personal Information.**

California residents have a right to limit our use and disclosure of sensitive personal information for any purposes other than to provide the services or goods you request or as otherwise permitted by law. GIC does not presently use or disclose sensitive personal information for any such additional purposes. However, if you would like to opt out of such uses or disclosures in the event we do in the future, you can do so and we will keep a record of this request.

To submit a request to limit the use and disclosure of your personal information, please email us at GrpLCD_PersonalData@gic.com.sg. You must use "California Request to Limit Sensitive Personal Information" in the subject line of your email and provide us with your full name and email address. In order to designate an authorized agent to act on your behalf, you must send a signed, written authorization containing your first name, last name, email address, and phone number to GrpLCD_PersonalData@gic.com.sg.

You can also write to us at the address above to submit your request by mail. Please include a heading or subject line "California Request to Limit Sensitive Personal Information" in your letter and provide us with your full name and email address.

4.4 **Right to Non-Discrimination**

We will not discriminate against you for exercising any of your CCPA Rights and we will not deny you goods or services, charge you a different price, or provide you with a lesser quality of goods or services if you exercise any of your CCPA Rights.

4.5 **Right to Notice / "Notice at Collection"**

At or before the time of collection of your personal information, you have a right to receive notice of our practices, including:

- the categories of personal information and sensitive personal information to be collected. Those details are provided in Section 1 of this Addendum.
- the purposes for which such information is collected or used. Those details are also provided in Section 1 above
- whether such information is sold or shared. As described in Section 4.2 above, we do not "sell" or "share" personal information as those terms are defined by the CCPA.
- how long such information is retained. The criteria used to determine how long we retain personal information are described in Section 3 above.

5. **Changes to This Addendum**

- 5.1 GIC reserves the right to amend this privacy addendum at our discretion and at any time. When we make changes to this privacy addendum, we will provide you with a copy of the updated notice and post the updated addendum on our website and update the addendum's effective date.

6. **Questions About This Addendum**

- 6.1 If you have any questions or comments about this notice or the ways in which GIC collects and uses your information, please contact:

Name: Lynn Hew Ooi Lyn

Email: lynnhew@gic.com.sg

Job applicants, vendors, members of the public and investment counterparties

Contact number: +65 6889 8377

Department: Legal and Compliance Department

Group Email: GrpLCD_PersonalData@gic.com.sg