

CONSOLIDATED UNDERTAKING FOR INDIVIDUALS

Date: 14 July 2023

To: GIC Private Limited ("GIC")

168 Robinson Road

#37-01 Capital Tower

Singapore 068912

UNDERTAKING TO SAFEGUARD CONFIDENTIAL INFORMATION

1. I, Vivekananthan Dhanasekaran
(**FIN** : G3927890T) of
Tampines Street 44, #04-269, Singapore 520481,

hereby agree and undertake, in consideration of GIC agreeing to enter into

AMENDMENT AGREEMENT No. 1 with
Keyteo Consulting Pte. Ltd.

("the Company") dated 13 July 2023 ("the Agreement") and in

consideration of GIC agreeing to furnish the Company and me Confidential

Information (as defined below) subsequent to the Effective Date (as defined in

paragraph 10 below), in connection with such Agreement, as follows:

(a) I will only use the Confidential Information solely for the purpose of
fulfilling the Company's obligations under the Agreement;

(b) I will treat the Confidential Information as private and confidential and
safeguard it accordingly;

- (c) I will not, without the prior written consent of GIC, disclose any Confidential Information to any person other than such person who has executed an undertaking in favour of GIC in such form acceptable to GIC and is authorised by the Company to receive such information in the performance of the Agreement, nor otherwise make use of any Confidential Information; and I shall prevent the publication or disclosure of any Confidential Information acquired, received or made by me, or made available to me;
- (d) All Confidential Information and copies thereof (in whatever form) which shall be acquired, received or made by me, or made available to me is and shall remain the property of GIC, and shall be surrendered by me to a person duly authorised by GIC at the termination of the Agreement, or at the request of GIC at any time during the term of the Agreement; and I shall destroy any other records (including, without limitation, those in machine readable form) containing Confidential Information acquired, received or made by me, or made available to me;
- (e) I shall not at any time, including after the date of termination of the Agreement, represent myself or permit myself to be held out by any person, firm or company as being in any way connected with or interested in the business of GIC and/or its subsidiaries and/or associated companies;

(f) I shall continue to be bound by the terms of this Undertaking notwithstanding the completion and/or termination of the Agreement; and

(g) I hereby acknowledge and agree that the matters stated in the above sub-paragraphs are reasonable and necessary in all circumstances to preserve and protect any Confidential Information.

2. In this Undertaking:

2.1 "Confidential Information" means all information relating to or to the activities of GIC and its subsidiaries and associated companies, including but not limited to:

(a) all information and documents relating to or in connection with or in respect of the business or operations and all financial and any other information of, GIC and/or its subsidiaries and/or associated companies and its or their dealings, transactions and affairs in whatsoever form whether in writing, in pictorial form, in machine readable form or otherwise including information perceived through aural or visual means; and

(b) all information and documents derived from any information or documents referred to in (a) above.

2.2 "Document" means all records, reports, documents, papers and other materials in whatever form originated by or on behalf of GIC and/or its subsidiaries and/or

associated companies relating to or in connection with or in respect of the business, operations and/or financing and any other information of GIC and/or its subsidiaries and/or associated companies and GIC's and/or its or their dealings, transactions and affairs.

3. If any Confidential Information (in the reasonable opinion of my legal counsel) is required to be disclosed under compulsion of law (whether by oral question, interrogatory, subpoena, civil investigative demand or otherwise) or by order of any court or governmental or regulatory body to whose supervisory authority I am subject, I shall promptly provide GIC with notice in writing of such requirement so that GIC may seek protective order or other relief. If GIC fails to obtain or does not obtain such an order or other relief, disclosure of the required information may be made pursuant to such requirement provided that I exercise my best efforts to obtain assurance that confidential treatment will be accorded to such information.
4. The obligations in this Undertaking do not apply to any information which is:-
 - (a) in the public domain other than as a result of breach of this Undertaking;
 - (b) given to me/ the Company by a third party not known by me/ the Company to be in breach of any confidentiality obligation to GIC;
 - (c) already in my or the Company's free possession at the time of disclosure.

UNDERTAKING TO SAFEGUARD OFFICIAL SECRETS ACT MATERIAL

5. I undertake and agree with GIC that:

- (a) I have read Sections 5 and 6 of the Official Secrets Act (Cap 213) (“OSA”) extracted as Appendix 1 which relates to (amongst other things) the safeguarding of documents and information described in Sections 5(1) and 6(2) and to my obligations under GIC’s rules and regulations on security and confidentiality as spelt out in the various policies provided by GIC and as set out in this Undertaking.
- (b) All OSA Material, including all documents and information acquired which I have obtained, has access to or worked on by me in the course of my deployment at GIC (regardless of their security classification), are strictly confidential and protected under the OSA (“Protected Material”). I will not publish, disclose or communicate Protected Material to any unauthorized recipients in any form, whether during or after my deployment at GIC, except with proper authority and in the course of my official duties.
- (c) I will take reasonable care and will not endanger the safety and secrecy of any Protected Material. I will not send any Protected Material to my personal email account and/or to any other unauthorised email account, as well as to any online file sharing services, USB storage devices and/or mobile devices. Any breach or neglect of this undertaking is a disciplinary offence and may also render me liable to prosecution under the OSA. The penalty for a breach of the OSA is a jail term of up to two years and/or a fine of up to S\$2,000.

UNDERTAKING TO COMPLY WITH GIC'S POLICIES AND STANDARDS

6. I undertake and agree to comply with GIC's policies and standards applicable to my deployment as may be provided by GIC from time to time (the "Applicable Policies"), including without limitation of the foregoing (i) GIC's Policy on Acceptable Use of Technology Resources (extracts from the current version of that policy attached as Appendix 2 for reference); and (ii) GIC Privacy Standard (the current standards are attached as Appendix 3 for reference), all as may be updated by GIC from time to time. I acknowledge that breaches of the Applicable Policies may constitute serious offences that, without prejudice to GIC's other remedies, GIC may report to the relevant authorities.

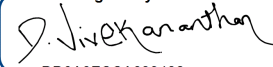
In furtherance of Section 6(ii), I agree and consent to the collection, use and processing of my facial image data for the purposes of accessing and ensuring the security of GIC's office premise(s). I acknowledge and agree that GIC's Privacy Standard (as attached) shall be applicable to the collection, use and processing of my facial image data for the aforementioned purposes.

ESIGN, GOVERNING LAW AND JURISDICTION

7. This Undertaking may be executed by way of original wet-ink signatures or electronic signatures as instructed by GIC. In the event this Undertaking is executed by electronic signatures, I agree that the electronic signature has the same binding effect as a physical signature. For the avoidance of doubt, I agree that the Undertaking, or any part thereof, shall not be denied legal effect, validity or enforceability solely on the ground that it is in the form of an electronic record.
8. I hereby acknowledge and agree that any breach of any provisions of this Undertaking could cause injury to GIC and/or its subsidiaries and/or associated companies, and that monetary damages would not be an adequate remedy. In the event of a breach or threatened breach by me, GIC shall be entitled to injunctive relief in any court of competent jurisdiction, and I shall reimburse GIC for all costs, claims, demands, liabilities or expenses of whatsoever nature arising directly or indirectly out of the breach or threatened breach. Nothing in this Undertaking shall be construed as prohibiting GIC from pursuing any other remedies available to it for a breach or threatened breach. By providing my personally identifiable information in this Undertaking (Name, NRIC/Passport, Address), I consent to GIC processing such information for the purposes of enforcing this Undertaking in the event of my breach or threatened breach of this Undertaking.
9. This entire Undertaking shall be governed by and construed in accordance with the laws of the Republic of Singapore. I hereby agree to submit to the non-exclusive jurisdiction of the Singapore courts.

10. The effective date of this Undertaking is 17 July 2023 (the “Effective Date”).

This Undertaking is signed on the day and year first above written.

DocuSigned by:

DD0A9FCCA633482...

Signed by Vivekananthan Dhanasekaran)
FIN G3927890T)

Appendix 1 – Official Secrets Act extracts

OFFICIAL SECRETS ACT (CHAPTER 213) Wrongful communication, etc., of information.

5.—(1) If any person having in his possession or control any secret official code word, countersign or password, or any photograph, drawing, plan, model, article, note, document or information which —

- (a) relates to or is used in a prohibited place or anything in such a place;
- (b) relates to munitions of war;
- (c) has been made or obtained in contravention of this Act;
- (d) has been entrusted in confidence to him by any person holding office under the Government; or
- (e) he has obtained, or to which he has had access, owing to his position as a person who holds or has held office under the Government, or as a person who holds, or has held a contract made on behalf of the Government or any specified organisation, or as a person who is or has been employed under a person who holds or has held such an office or contract,

does any of the following:

- (i) communicates directly or indirectly any such information or thing as aforesaid to any foreign Power other than a foreign Power to whom he is duly authorised to communicate it, or to any person other than a person to whom he is authorised to communicate it or to whom it is his duty to communicate it;
- (ii) uses any such information or thing as aforesaid for the benefit of any foreign Power other than a foreign Power for whose benefit he is authorised to use it, or in any manner prejudicial to the safety or interests of Singapore;

- (iii) retains in his possession or control any such thing as aforesaid when he has no right to retain it, or when it is contrary to his duty to retain it, or fails to comply with all lawful directions issued by lawful authority with regard to the return or disposal thereof; or
- (iv) fails to take reasonable care of, or so conducts himself as to endanger the safety or secrecy of, any such information or thing as aforesaid,

that person shall be guilty of an offence.

(2) If any person receives any secret official code word, countersign, password, or any photograph, drawing, plan, model, article, note, document or information knowing, or having reasonable ground to believe, at the time when he receives it, that the code word, countersign, password, photograph, drawing, plan, model, article, note, document or information is communicated to him in contravention of this Act, he shall be guilty of an offence unless he proves that the communication to him of the code word, countersign, password, photograph, drawing, plan, model, article, note, document or information was contrary to his desire.

(3) In any proceedings against a person for an offence under this section, where it is proved that that person is or has been in the employment or service of any foreign Power or government in breach of any undertaking which he has made with the Government or any specified organisation, he shall be deemed to be in possession or control of such information or thing as is referred to in subsection (1) and to have unlawfully communicated that information to a foreign Power or to have used that information or thing in a manner prejudicial to the safety or interests of Singapore.

(4) In subsection (3), “undertaking” means any undertaking in writing which a public officer or any other person has made with the Government or any specified organisation whereby the officer or person undertakes not to serve or be employed by any foreign Power or government within a specified period after his retirement or resignation from the public service or that specified organisation or otherwise unless he has obtained the prior approval of the Government or that specified organisation.

Unauthorised use of uniforms, falsification of reports, forgery, personation and false documents

6.—(1) If any person gains or assists any other person to gain admission to a prohibited place otherwise than by an authorized point of entry or, for the purpose of gaining admission, or of assisting any other person to gain admission, to a prohibited place, or for any other purpose prejudicial to the safety or interests of Singapore within the meaning of this Act –

[...]

(c) orally, or in writing in any declaration or application, or in any document signed by him or on his behalf, knowingly makes or connives at the making of any false statement or any omission;

[...]

he shall be guilty of an offence.

(2) If any person —

(a) retains for any purpose prejudicial to the safety or interests of Singapore any official document, whether or not completed or issued for use, when he has no right to retain it, or when it is contrary to his duty to retain it, or fails to comply with any directions issued by any Government department or any

specified organisation or any person authorised by that department or specified organisation with regard to the return or disposal thereof;

- (b) allows any other person to have possession of any official document issued for his use alone, or communicates any secret official code word, countersign or password so issued, or, without lawful authority or excuse, has in his possession any official document or secret official code word, countersign or password issued for the use of some person other than himself, or on obtaining possession of any official document by finding or otherwise, neglects or fails to restore it to the person or authority by whom or for whose use it was issued, or to the Deputy Commissioner of Police;
- (c) without lawful authority or excuse, manufactures or sells, or has in his possession for sale, any such key, badge, device, die, seal or stamp as aforesaid; or
- (d) with intent to obtain an official document, secret official code word, countersign or password, whether for himself or for any other person, knowingly makes any false statement,

he shall be guilty of an offence.

Appendix 2 – GIC’s Policy on Acceptable Use of Technology Resources

1. INTRODUCTION

1.1 BACKGROUND

GIC regards information as a valuable asset, and its information processing systems as critical to its business. It is thus of utmost importance to protect these technology resources against unauthorised disclosure, modification, destruction or usage, which could lead to financial, regulatory/legal and/or reputational impact to GIC.

1.2 OBJECTIVE

This document sets out the expected user behaviour with regards to the usage of GIC information assets, as well as the software applications and hardware which store, transmit, process and/or display these assets.

1.3 SCOPE

This Policy applies to all users of GIC technology resources. Where there are stricter requirements stated in other GIC policies or standards, those requirements shall prevail over the minimum requirements stated in this Policy.

1.4 COMPLIANCE

1.4.1 All users shall conduct their activities in accordance with this Policy’s requirements. GIC employees who engage third parties provided with access to technology resources shall ensure that they are made aware of this Policy as well.

1.4.2 Management reserves the right to monitor the usage of GIC-owned technology resources, inspect the activities of users for any suspected abuse, unauthorised or illegal activities to ensure compliance with this Policy, and to disclose such information where it deems it necessary.

1.5 DEFINITIONS

GIC information	Any data created for the purpose of supporting GIC's business that has not been published publicly.
Technology resources	GIC information assets and any platform, device, network or tool used to access these assets.
Users	Personnel who are granted access to GIC technology resources, regardless of employment type.
Paid subscriptions	Any subscription-based information service which is paid for by GIC for usage by GIC staff members.
Management	GEC Members and Department Directors.
Communication systems	Systems or applications used primarily for communication purposes. These include email systems, instant messaging applications, audio/video conferencing systems, etc.
Social media	Applications on mobile or web-based technologies that allow users to create, share and exchange contents and media Examples include social networking sites (such as Facebook, Instagram, LinkedIn, Twitter, etc.), video and photo sharing websites, micro-blogging, weblogs, forums and discussion boards, etc.
End-user computing	Computing device capable of transmitting packet data either

device	directly (through the GIC network) or via connection to external network services (e.g. WiFi hotspots or cellular data networks).
Storage media	Hardware that stores data. Examples include CDs, DVDs, hard drives, thumb drives, flash memory devices, SD cards, compact flash cards, tapes, etc.
Remote access	The ability to access GIC information over a publicly accessible communication channel, e.g. Internet.

2. USER RESPONSIBILITIES

2.1 GENERAL TECHNOLOGY USAGE

2.1.1 Users shall use GIC technology resources and paid subscriptions only for GIC work- related purposes. While the use of corporate Internet/Intranet, email and instant messaging systems for personal communications is permitted, users shall ensure such systems are used primarily for work purposes, and that any personal use of such systems does not interfere with his/her duties or with GIC's business or systems.

[...]

2.1.4 Users shall only access data, applications or systems with valid authorisation and management approval. Unless authorised, the ability to connect to other systems does not imply the right to access these systems.

2.1.5 Users shall not use GIC technology resources and paid subscriptions for:

- (a) Personal business activities (revenue-generating or otherwise)
- (b) Inappropriate activities, such as pornography, fraud, defamation, breach of copyright, impersonation, unlawful discrimination, obscenity, racism, harassment, stalking, privacy violations, downloading of unauthorised software and illegal file sharing, software or media piracy

2.1.6 Users shall not attempt to, or through negligence, allow any other user to circumvent the security of GIC technology resources. This includes, but is not limited to:

- (a) Unauthorised application code decompilation/reverse engineering
- (b) Gaining access to system login credentials using brute-force methods

2.2 PASSWORD SECURITY

2.2.1 Users shall be held accountable for the security of accounts and passwords assigned to them. Users shall not divulge account passwords which have been issued to them. Such passwords shall not be stored or transmitted in clear text or displayed publicly.

[...]

2.2.3 In the event of suspected password compromise, users shall change their password and inform Technology Group (TG) Helpdesk immediately.

[...]

2.2.5 Users shall only be granted system access on a “need-to” basis, and inform the business owner when system access is no longer required.

2.3 END-USER COMPUTING DEVICE SECURITY

2.3.1 Users shall protect GIC information processed or stored on end-user computing devices (even if they are not GIC-owned) from unauthorised access. Users are encouraged to enable password/biometric authentication and individual user accounts on non GIC-owned end-user computing devices where technically feasible.

2.3.2 Users shall ensure these non GIC-owned end-user computing devices are kept physically secure, and are protected by consumer-grade system security software (e.g. anti-virus, anti-malware, personal firewall, etc.).

2.3.3 Users shall exercise due care while accessing GIC information in public places. Users shall always log out of active sessions after accessing GIC technology resources from public locations e.g. Internet cafes, airport lounges, etc.

2.3.4 Users shall ensure that screen lock is enabled whenever end-user computing devices are left unattended.

2.3.5 Users shall only print GIC information from authorised end-user computing devices, and to printers located in trusted locations. Hard copies shall be handled in accordance with the GIC Information Handling Procedures.

2.3.6 Users shall not make unauthorised hardware/software modifications on GIC-issued end-user computing devices.

2.3.7 Users shall report all IT security incidents to TG Helpdesk immediately. Examples of IT security incidents include: denial of service, unauthorised access/usage of GIC information, malware/virus infections, loss or theft of GIC-issued end-user computing devices, etc.

2.4 EMAIL AND OTHER COMMUNICATION SYSTEMS

2.4.1 Users shall exercise due care when sending emails and instant messages to ensure that the addressee(s) is/are the intended recipient(s). Users shall follow the Misdirected Email Handling Procedures when an email has been sent to unintended recipient(s).

2.4.2 Users shall exercise due care upon receiving email/attachment or click on links from suspicious/unknown sources. Users shall report suspicious emails to TG Helpdesk immediately.

2.4.3 Usage of public communication systems (e.g. WhatsApp, WeChat, etc.) to transmit GIC information in support of/relating to GIC's investment and operational activities (e.g. specific discussions related to potential or existing investments, conversations which identify specific business transactions, negotiations with vendors, client-related matters, etc.) is strictly prohibited.

2.4.4 Usage of such public communication systems for other business purposes not described in Section 2.4.3 shall be subject to relevant risk assessments, which shall include evaluating the presence and applicability of traceability, auditing, record keeping and access control features in the systems, as well as appropriate risk mitigation measures and/or risk acceptance decisions. Explicit authorisation by pre-designated approvers based on the risk assessment outcome shall be obtained before users can proceed to use these public communication systems.

2.4.5 Users shall not engage in the following activities:

- (a) Transmit or store any content that are likely to cause embarrassment or legal/reputational issues to GIC
- (b) Spam an individual, group or email systems with numerous or large emails

2.5 INTERNET, GIC INTRANET & SOCIAL MEDIA

2.5.1 Users shall be personally accountable for the contents they publish on the Internet/GIC Intranet/social media sites.

2.5.2 Users shall not post content that could reflect negatively on GIC, fellow colleagues or clients, or violate the privacy rights of others on the Internet/social media sites.

2.5.3 Users shall not engage in the following activities while using GIC technology resources to access the Internet/GIC Intranet:

- (a) Deface websites
- (b) Access Internet sites containing obscene, hateful, pornographic, gambling or otherwise illegal material for personal purposes
- (c) Publish any obscene, discriminatory, defamatory, harassing, racist comments or offending remarks on religion
- (d) Download and use copyrighted materials belonging to third parties from the Internet unless the necessary permissions or licenses have been obtained, and the downloading activity and use of such material is in compliance with the applicable terms and conditions of the Internet sites from which the copyrighted material is downloaded
- (e) Re-publish GIC information that has been shared within GIC Intranet sites to public Internet websites

2.6 PUBLIC/EXTERNAL STORAGE MEDIA

2.6.1 Users shall not store GIC information on external storage media unless explicitly pre-authorised to do so by designated approvers.

2.6.2 Users shall not store GIC information on public file storage services unless explicitly pre-authorised to do so by designated approvers.

2.6.3 Users shall ensure that external storage media is free from viruses/malware prior to use on GIC- issued end-user computing devices.

2.6.4 Users shall keep external storage media containing GIC information physically secure.

2.7 SOFTWARE USAGE

2.7.1 Users shall adhere to the software request process stipulated by TG if they need to use any software not in TG's Approved Software List.

2.7.2 Users shall not copy, download, install, use or distribute unauthorised software as this may infringe intellectual property rights law or introduce viruses/malware into GIC's network.

2.7.3 Users shall not tamper with the software installed on GIC technology resources, or do any acts which would constitute an infringement of the copyright of the software proprietors.

2.8 REMOTE ACCESS

2.8.1 Users shall not allow their remote access to be used by other personnel. Users shall log off their remote sessions after use or lock the screen when leaving their end- user computing devices unattended.

2.8.2 Users shall exercise due care in protecting the security of software/hardware tokens issued to them to facilitate remote access.

2.9 NETWORK SECURITY

2.9.1 Users shall not share their connection (e.g. Internet tethering) to the GIC network with other personnel.

2.9.2 Users shall not engage in the following activities:

- (a) Exploit or probe for security vulnerabilities in the GIC network or other organisations' networks without authorisation from TG management
- (b) Deliberately introduce any form of computer virus or malware into the GIC network

Appendix 3 – GIC Privacy Standard

GIC'S PRIVACY STANDARD FOR HANDLING PERSONAL DATA

GIC respects the privacy of individuals and is deeply committed to protecting the personal data of individuals in our possession, custody and control. GIC is also accountable under the applicable personal data protection laws and regulations to put in place appropriate and adequate policies, procedures, systems and controls and to maintain records to demonstrate our compliance.

Maintaining the highest standards in GIC's handling of personal data is both a collective and an individual responsibility, and this set of Privacy Standard ("**Standard**") addresses how GIC and its employees¹ should collect, use, store, delete or otherwise process personal data. The Standard includes a broad summary of the key data protection obligations that apply to GIC, and as employees, you are required to understand and adhere to this Standard in relation to any personal data that you access in the course of your work. You may also be required to attend training in relation to this Standard and related policies.

A breach of this Standard may give rise to disciplinary action as set out in Chapter 2 of the Compliance Manual and in accordance with GIC's Conduct Framework.

Quick Links

- [1. The Importance of Compliance](#)
- [2. Definitions](#)
- [3. Personal Data Protection Principles](#)
- [4. Lawfulness, fairness and transparency](#)

- [5. Purpose limitation and data minimisation](#)
- [6. Accuracy and record keeping](#)
- [7. Storage limitation](#)
- [8. Integrity and confidentiality](#)
- [9. Special categories of personal data and criminal records data](#)
- [10. Sharing personal data](#)
- [11. Data subject rights](#)
- [12. Data breach procedure](#)
- [13. Useful contact details](#)

1. The Importance of Compliance

- 1.1 The implications of data privacy breaches are severe. Global personal data protection laws, including the EU General Data Protection Regulation (“**GDPR**”), impose significant fines against organisations for data privacy breaches. For example, under the EU GDPR and depending on the type of the breach, organisations may be fined up to the higher of €20 million or 4% of total worldwide annual turnover of the organisation. Individuals can also be personally liable for data protection breaches. Therefore, it is important for GIC to be able to demonstrate and evidence compliance with data privacy laws.

2. Definitions

¹ This group includes, but is not limited to, contractors and vendor staff. Departments that are engaging vendors should ensure, on a best efforts basis, that the vendor staff are aware of and adhere to this set of Standard.

“personal data” means information relating to a living individual who can be identified from that information (or from that information when combined with other information in our possession).

Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal);

“processing” means any activity that involves the use of personal data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties;

“special categories of personal data” (sometimes known as sensitive personal data) means data about a person’s racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership(s), physical or mental health, sex life or sexual orientation, and their biometric data or genetic data. It may include other data set such as criminal offences, convictions, social security numbers which are dictated by the relevant regulation as requiring a higher level of protection by GIC.

3. Personal Data Protection Principles

- 3.1 GIC is committed (and we expect all our employees to be similarly committed) to data protection in compliance with the following requisite legal principles:

1.	We will process personal data lawfully, fairly and in a transparent manner.
2.	We will only collect personal data for specified, explicit and legitimate purposes. We will not process it in a manner that is incompatible with those purposes.
3.	We will only process personal data that is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

4.	We will ensure that personal data is accurate and, where necessary, kept up to date. Where it is inaccurate, we will take every reasonable step to ensure that it is corrected or erased without delay, taking into account the purposes for which it is processed.
5.	We will refrain from keeping personal data in a form which permits identification of the individual to whom it relates for any longer than is necessary for the purposes for which it is processed.
6.	We will use appropriate technical or organisational measures to ensure the security of personal data, which will include its protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

4. Lawfulness, fairness and transparency

4.1 We may only process personal data where we have a lawful basis for doing so – the lawful bases on which we can process personal data are set out in the relevant data protection legislation and include, by way of example only:

- 4.1.1 the individual has given his/her consent;
- 4.1.2 it is necessary for the performance of a contract that we have with the individual;
- 4.1.3 it is necessary for us to comply with the law; or
- 4.1.4 it is necessary to further our legitimate interests or the legitimate interests of a third party (unless these are overridden by the interests or fundamental rights and freedoms of the individual).

4.2 Before we start to process personal data (for example, before we collect personal information from an individual), we should consider our reasons for collecting the information and why we need it. We must also identify and document the legal basis which permits us to obtain and process that information lawfully. You should check in with your [Department Personal Data Representative](#) (“PD Rep”) in case of any doubt.

- 4.3 We will provide any individual whose personal data we process with a data privacy notice or direct the individual to the applicable personal data protection policy, which sets out certain specific details which we are required by law to include, such as how and why we use their personal data, the basis on which our processing is lawful, and their rights in relation to their personal data.

5. Purpose limitation and data minimisation

- 5.1 We will only process personal data that is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
- 5.2 We should only process personal data for the specific purposes that we have identified, and that have been expressly notified to the individual in our personal data protection policies and/or data privacy notice. We must not use personal data for new or different purposes from that already advised to the individual.
- 5.3 You should not obtain any personal information from an individual beyond that required for your work.

6. Accuracy and record keeping

- 6.1 We will ensure that personal data that we collect is accurate and where necessary kept up to date; where it is inaccurate we will take every reasonable step to ensure that it is corrected or erased without delay, taking into account the purposes for which it is processed.
- 6.2 The accuracy of personal data should be checked at the point it is collected and kept up to date thereafter.

- 6.3 If you become aware that any personal data that we process is inaccurate, you must inform your manager and take reasonable steps to amend it or erase it (as appropriate) taking into account the requirements of GIC's Record Retention Policy where appropriate.
- 6.4 You must also assist, if required, with our maintenance of appropriate records in relation to our handling of personal data.

7. Storage limitation

- 7.1 We will take all reasonable steps and refrain from keeping personal data in a form which permits identification of the individual to whom it relates for any longer than is necessary for the purposes for which it was originally collected or processed. GIC's [Record Retention Policy](#) sets out the duration of our retention of information containing personal data or the criteria that we will use to determine the relevant period.
- 7.2 After the expiry of the applicable retention period, unless there is a sound business reason to retain the personal data (for example, an individual has brought a claim against GIC and the retained personal data is relevant to the case), it should be disposed of securely and destroyed effectively in accordance with guidance from your manager / PD Rep / LCD's Personal Data Protection Team.

8. Integrity and confidentiality

- 8.1 We will ensure we comply with GIC's policies and controls to ensure the security of personal data that we hold, which will include its protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

8.2 Where a type of processing (e.g. using new technologies or the processing of biometric data) is likely to result in a high risk to individuals, we must carry out an assessment of the impact of the envisaged processing operations.

8.3 You are required to adhere to applicable corporate policies to protect the integrity and confidentiality of the personal data which we process and to which you have access. You must take particular care to protect special categories of personal data.

8.4 In practice, this means that you must:

8.4.1 only access the personal data that you are permitted to access by virtue of your role for authorised purposes;

8.4.2 not allow any other person (including other GIC employees) to access personal data unless you know that they are authorised and have a need-to-know basis to access the data;

8.4.3 keep personal data secure (for example, by complying with GIC's policies on system access, password protection, encryption and secure file storage and destruction);

8.4.4 not remove personal data (including personal data in files), or devices containing personal data (or which can be used to access it), from GIC's premises or systems unless you are authorised to do so or appropriate security measures are in place (such as pseudonymisation, encryption or password protection); and

8.4.5 not store personal data on local drives or on personal devices used for work purposes.

9. Special categories of personal data and criminal records data

9.1 From time to time, we may need to process special categories of personal data and criminal records data. We must only process such personal data where we have a

lawful basis for doing so. Please only proceed with such processing after you have engaged LCD's Personal Data Protection Team.

10. Sharing personal data

10.1 Generally, you should not share personal data with any third parties unless certain safeguards and specific contractual arrangements are in place. Your manager/ PD Rep will be able to confirm this.

11. Data subject rights

11.1 You should be aware of the rights that individuals (including you) have in relation to their personal data, which are summarised below:

11.1.1 If individuals have given their consent to processing, they may withdraw it at any time (and this must be as easy for them to do as it was to give consent in the first place);

11.1.2 Individuals have the right to be provided with clear, transparent and easily understandable information about how their personal data is used and their rights; 11.1.3 Individuals are entitled to access their personal data;

11.1.4 Where we hold personal data that is inaccurate or incomplete, individuals are entitled to ask us to rectify or complete such data, and in certain circumstances to erase it;

11.1.5 Individuals are entitled to restrict some processing of their personal data, which means asking us to limit what we do with it;

11.1.6 Individuals are entitled to object to our processing of their personal data in certain circumstances, including where processing takes place in pursuance of GIC's legitimate business interests;

11.1.7 Individuals are entitled to data portability in certain circumstances, which means the right to obtain from us and re-use their personal data for their own purposes;

11.1.8 Individuals are entitled not to be subject to automated decision making where this has legal or other significant consequences for them, except where they have explicitly consented or where it is necessary for entering into or performing a contract with them; and

11.1.9 individuals may submit a complaint to the relevant Data Protection Authority about our processing of their personal data, although we would always encourage anyone to bring any concerns to our attention first, so that we can try to resolve them.

11.2 If you become aware that an individual would like to exercise any of these rights (or if you would like to exercise any of these rights), you should speak to LCD's Personal Data Protection Team. Appropriate steps may need to be taken to verify the identity of the person making the request.

12. Data breach procedure

12.1 A data breach is *"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed"*.

12.2 A breach does not necessarily mean that personal data is disclosed externally without the relevant authorisation; it could mean that it has been accessed internally by someone without the relevant permission.

12.3 If the compromised data consists of or includes personal data, there may be a legal and regulatory obligation to notify the relevant Data Protection Authority and the affected individuals. In certain jurisdictions, there is a requirement to make mandatory notifications to the authority within a prescribed time period.

12.4 Please report any known or suspected data breach to LCD's Personal Data Protection Team as soon as it occurs, even if you are not sure whether a breach has in fact occurred or not, so that we can make the relevant assessment on whether any reporting obligations may arise and take appropriate action as necessary.

13. Useful contact details

13.1 For questions relating to this Standard, please email LCD's [Personal Data Protection Team](#) (GrpLCD_PersonalData).