DATA PROCESSING AGREEMENT

FOR A GARRISON ULTRA® SERVICE

These Data Processing Terms and Conditions ("**DPA**") are an integral part of the Agreement for the provision on a trial or commercial basis of the Garrison ULTRA® Service and are a legal agreement between the relevant Garrison entity as set out in the Order ("**Garrison**") and the legal entity being provided access to and making use on a trial or commercial basis of the Garrison ULTRA® Service ("**Customer**"). Each a "Party" and together the "Parties".

1 Definitions

In this Agreement, unless the context otherwise requires, the following words shall have the following meanings:

Agreement	means the contract between Garrison and Customer for the provision on a trial or commercial basis of the Garrison ULTRA® Service to which this DPA is incorporated.
Data Controller	means Garrison in respect of Customer organisational data including name, organisation, job, email address and phone numbers; and Customer in respect of all other personal data set out in Appendix A.
Data Processor	means Garrison in respect of all personal data set out in Appendix A for which Garrison is not the Data Controller.
Data Protection Laws	means any laws, regulations, guidelines, and/or codes of practice that: (a) are applicable to data processed by Data Processor regardless of jurisdiction or location; and (b) govern the collection, use, processing, storage, transfer, and protection of Personal Data or personal information. Data Protection Laws include the General Data Protection Regulation 2016/679 (EU) (**"GDPR"**), Privacy and Electronic Communications Directive 2002/58 (EU), Data Protection Act 2018 (UK) (**"UK-GDPR"**), Privacy and Electronic Communications (EC Directive) Regulations 2003 (UK), California Consumer Privacy Act 2018 (California) (**"CCPA"**), and the Personal Data Protection Act 2012 (Singapore) (**"PDPA"**). The terms **"breach"**, **"data subject"**, **"processing"**, and **"sensitive personal data"** shall have the same meaning as in and for Data Protection Laws.
Garrison Affiliates	means any entity that controls, is controlled by or is under common control with Garrison, where "control" means ownership of more than fifty percent of the outstanding securities representing the right to vote for the election of directors or other managing authority.
Garrison ULTRA® Service	means the web isolation service provided by Garrison to Customer under the Agreement.
Personal Data	means information that identifies, relates to, describes, or is capable of being associated with a natural person, i.e., personal data as defined by Data Protection Laws, arising out of or in connection with the Subject Matter, including as set out in the Appendix A. Personal Data includes "sensitive personal data" as defined by Data Protection Laws.
Subject Matter	means: (i) for the provision of Garrison ULTRA® to Customer pursuant to the Agreement; (ii) for each Party to meet their respective obligations as set out in this DPA; and (iii) to comply with any legal obligation to which either Party is subject.

2 Data Processing

2.1 In processing Personal Data on behalf of the Data Controller, unless otherwise required by applicable law the Data Processor shall:

a) Comply with all applicable Data Protection Laws;

b) Process Personal Data solely for the Subject Matter, and only to the extent necessary for the Subject Matter;

c) Process Personal Data in accordance with the instructions of the Data Controller;

d) Implement and maintain appropriate technical and organisational measures to ensure the security, confidentiality, and integrity of Personal Data, taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of processing as set out in Appendix B;

e) Ensure that all personnel who have access to Personal Data are subject to confidentiality obligations and have received appropriate training on data protection; and

f) Permanently delete Personal Data promptly upon receipt of a written request by the Data Controller.

2.2 Customer acknowledges and agrees that Garrison may process data that has been fully and irreversibly anonymised and aggregated for its own internal business purposes including for the purpose of analytics and/or to improve the Garrison ULTRA® Service.

3 Impact Assessments and Prior Consultation

3.1 Data Processor taking into account the nature of the processing, and the information available to it, shall provide reasonable assistance to Customer with any data protection impact assessments, and prior consultations with competent data privacy authorities, which Data Controller reasonably considers to be required by Data Protection Laws.

4 Data Subject Requests

4.1 Data Processor shall promptly notify Customer if it receives a request from a data subject under Data Protection Laws. Data Processor shall assist the Data Controller to comply with any request for access, correction or removal of Personal Data required by Data Protection Laws.

5 Unauthorised Processing

5.1 Data Processor shall notify the Data Controller promptly upon becoming aware of any unauthorised or unlawful processing, accidental or unlawful loss, destruction, alteration, or disclosure of Personal Data.

6 Data Breach

6.1 Data Processor shall cooperate with the Data Controller to investigate and remediate any data protection incident, including any required notifications to data protection authorities or affected data subjects.

7 International Data Transfers

7.1 Data Controller consents to the transfer by the Data Processor of Personal Data originating within a State to other States subject to compliance with the requirements for cross-border data transfers in any applicable Data Protection Laws and this clause. The Data Processor shall ensure that all cross-border transfers of Personal Data are conducted pursuant to a mechanism then considered to comply with applicable Data Protection Law requirements for cross-border transfers, including for Personal Data originating within:

a) European Economic Area, that the transfer is: (i) to a State the subject of an adequacy decision by the European Commission, or (ii) pursuant to standard contractual clauses set out in Commission Implementing Decision (EU) 2021/914 ("SCC") which are incorporated into a written contract between the Data Processor and the recipient;

b) United Kingdom, that the transfer is: (i) to a State the subject of an adequacy decision by the UK Government, (ii) pursuant to standard contractual clauses set out in the International Data Transfer Agreement 2022 which are incorporated into a written contract between the Processor and the recipient, or (iii) pursuant to the International Data Transfer Addendum 2022 addended to the SCC which are together incorporated into a written contract between the Data Processor and the recipient;

c) Singapore, that the transfer is to a State that provides a standard of data protection comparable to that provided under the PDPA; or

d) California, that the transfer is: (i) pursuant to a written agreement with the recipient requiring the same level of data protection as required by the CCPA, or (ii) to a recipient that is certified under an approved certification mechanism.

8 Sub-Processors

8.1 Controller authorises Data Processor to pass Personal Data to sub-processors, including those identified in Appendix A, subject to compliance by the Processor with the terms of this DPA.

9 Audit Rights

9.1 Data Controller shall have the right to audit Data Processor's compliance with this DPA. Such audit may be performed once per calendar year, at Data Controller's expense, on at least 30 days prior written notice, during normal business hours, in a manner that does not unreasonably interfere with normal operations, and without compromising any confidential or proprietary information.

10 Miscellaneous

10.1 In this DPA reference to any: (a) statute or statutory provision is a reference to it as amended, extended, or re-enacted from time to time, and any subsidiary legislation and/or subordinate instrument made under it; (b) person includes natural persons, companies, partnerships, associations, governments, organisations, states, government or state agencies, foundations, charities, and trusts; (c) company shall include any company, corporation, or other body corporate, wherever and however incorporated or established; and (d) Party includes a reference to that Party's successors in title, permitted assignees and transferees.

10.2 In this DPA: (a) words denoting the singular shall include the plural and words denoting the plural shall include the singular; (b) headings are for convenience only and do not affect the interpretation of this Agreement; and (c) the word "including", and similar expressions will not be construed as words of limitation and shall be read as "including, but not limited to".

10.3 No Party may assign this DPA to any other person without the prior written consent of the other Party, such consent not to be unreasonably withheld, delayed, or conditioned. Any purported assignment in breach of this clause shall be deemed null and void.

10.4 This DPA constitutes the entire agreement between the Parties on matters of data protection and supersedes and merges all prior discussion and any prior agreement. Each Party acknowledges that in entering into this DPA it has not relied on any warranty, representation or other promise of any nature not contained in this DPA.

10.5 This DPA and any disputes arising out of or in connection with it or its subject matter shall be construed in accordance with and governed exclusively by the laws of England and the acts of the Parliament of the United Kingdom which are applicable in England.

10.6 The Parties irrevocably agree the courts of England and Wales shall have exclusive jurisdiction to settle any claim that arises out of or in connection with this DPA or its subject matter.

APPENDIX A – DATA PROCESSING FOR THE GARRISON ULTRA® SERVICE

Type of Personal Data	Category of Data Subject	Purpose	Nature	Duration	Garrison	Customer	Sub-Processors?	Transferred outside Customer home region?
Customer organisational Data (e.g., name, organisation, job, email address and phone numbers)	Customer representatives	Service management, customer communication, including notification of software updates. Contract management. Feature improvements and product marketing	Data stored on CRM system; email systems; files on corporate network/intranet	For the duration of the Agreement, though details may be updated by Customer from time to time. Commercial contacts may be retained for a further 6 (six) years for contract management purposes	Data Controller	Data Controller	Garrison Affiliates	Yes
Username, email address, first and last name, and role in Customer organisation	Customer designated administrators and Authorised Users	For designated Customer administrators to manage the service in the Garrison ULTRA® Portal For Authorised Users to log into Garrison ULTRA®	Data stored and encrypted by AWS	For 36 (thirty-six) months from expiry or termination of the Agreement or Customer's request of deletion of the license created for Access whichever occurs earlier	Data Processor	Data Controller	Garrison Affiliates	Customer must choose the home region of their choice at the start of onboarding If the elected home region is not where the Customer designated administrator is located, this will necessitate a transfer to a third country
Logs of Customer designated administrators performing actions in the Garrison ULTRA® portal	Customer designated administrators for the Garrison ULTRA® portal	For Customer monitoring of Customer designated administrators For provision and management of Garrison ULTRA® by Garrison	Data stored and encrypted by AWS	For 36 (thirty-six) months from when logs are generated	Data Processor	Data Controller	Garrison Affiliates	Customer must choose the home region of their choice at the start of onboarding If the elected home region is not where the Customer designated administrator is located, this will necessitate a transfer to a third country

Type of Personal Data	Category of Data Subject	Purpose	Nature	Duration	Garrison	Customer	Sub-Processors?	Transferred outside Customer home region?
Authorised User browsing data generated *during the active browsing session* including Cookies, Browsing History, Passwords, Downloaded Files Downloaded Files may include sensitive Personal Data	Authorised Users plus Personal Data of other Data Subjects that may exist within their browsing activity or downloads	For the provision of Garrison ULTRA®	Data processed on the Garrison node during the browsing session	All Browsing data is securely wiped from the Garrison node at the end of a session and cannot be accessed by anyone except the Authorised User that is currently on the node	Data Processor	Data Controller	Garrison Affiliates	Yes – an active session will ordinarily be in the region the Authorised User is in at the time of commencing a session Each region may contain data centres in multiple countries and from time to time a different region may be used for operational purposes
Authorised User browsing data generated *across browsing sessions* including Cookies, Browsing History, Passwords, Downloaded Files Downloaded Files may include sensitive Personal Data	Authorised Users plus Personal Data of other Data Subjects that may exist within their browsing activity or downloads	For the provision of Garrison ULTRA® and in particular for seamless browsing activity between browsing sessions	Data processed on the Garrison node during the browsing session and then data stored in an encrypted format in AWS. The storing of the data is subject to the relevant feature being enabled by the Authorised User. The data is transferred to a node and decrypted at the start of a session. The encryption key that is used is generated from a combination of the user ID and a per-customer secret. The per- customer secret is maintained in a separate AWS database and is itself encrypted	Browsing data at rest will be retained for 6 (six) months from when it was last accessed by the Authorised User unless Customer requests deletion or Authorised User deletes it during a live browsing session	Data Processor	Data Controller	Garrison Affiliates and AWS	Yes - for performance reasons data may be replicated between regions using the same encryption standards Customer has the ability to activate or deactivate regions of their choice.
Authorised User browsing logs from native browser (if Customer's designated administrator configures and enables the Trust Qualified Browsing feature in the Garrison ULTRA® Customer portal)	Authorised Users	For the provision of Garrison ULTRA®	Data stored and encrypted by AWS	For 36 (thirty-six) months from when logs are generated	Data Processor	Data Controller	Garrison Affiliates and AWS	Customer must choose the home region of their choice at the start of onboarding If the elected home region is not where Authorised User is browsing from, this will necessitate a transfer to a third country

Type of Personal Data	Category of Data Subject	Purpose	Nature	Duration	Garrison	Customer	Sub-Processors?	Transferred outside Customer home region?
Authorised User browsing logs within Garrison ULTRA® URLs directly and indirectly (if indirect URLs are enabled) visited by Authorised User, including username, URL, time of request and whether it was direct or not	Authorised Users	For Customer monitoring and control of corporate internet use	Data stored and encrypted by AWS	For 7 (seven) days from when the logs were generated.	Data Processor	Data Controller	Garrison Affiliates and AWS	Customer must choose the home region of their choice at the start of onboarding If the elected home region is not where Authorised User is browsing from, this will necessitate a transfer to a third country
Authorised User browsing logs and administrator actions logs	Authorised Users and Customer designated administrators	Customer can export logs from Garrison ULTRA® into its own environment for Customer's own storage and analysis purposes	If Customer chooses to export logs from Garrison ULTRA®, the logs are exported to Customer's environment either via a management API or a Garrison provided log connector	Once logs are exported to Customer's environment, Customer is solely responsible for those logs. In accordance with the previous row of this Appendix, Garrison retains copies of the logs for 7 (seven) days from when the logs were generated	Data Processor	Data Controller	Garrison Affiliates and AWS	If Customer chooses to transfer the logs outside Garrison ULTRA® the location is solely within Customer's control
Any content (e.g. text and images etc.) that can be copied or printed by Authorised Users from the Internet using Garrison ULTRA®	Authorised Users	For the provision of Garrison ULTRA® and in particular for enabling copy / paste and printing functionality of text and images	Content viewed as part of Authorised User Browsing data that can be copied or printed This data is securely transferred through a Garrison Transfer Appliance and then via AWS to the Authorised User's local device	Content is securely wiped from the Garrison Transfer Appliance and AWS after the transfer is made	Data Processor	Data Controller	Garrison Affiliates and AWS	Customer must choose the home region of their choice at the start of onboarding The transfer will move from where Authorised User is browsing from, through the elected home region and then onward to where Authorised User physically is

Type of Personal Data	Category of Data Subject	Purpose	Nature	Duration	Garrison	Customer	Sub-Processors?	Transferred outside Customer home region?
Any content (e.g. text and images etc.) that can be copied by Authorised Users to the Garrison ULTRA® isolated environment from Customer Environment	Authorised Users	For the provision of Garrison ULTRA® and in particular for enabling copy / paste functionality of text and images	Content stored in Authorised User clipboard This data is securely transferred from Authorised User's local device to the Garrison ULTRA® isolated environment Once in the Garrison ULTRA® isolated environment, the data is no longer in the Customer Environment and therefore is exposed to potential risk This functionality is enabled by default The Garrison ULTRA® Service does not inspect this content and Garrison expressly disclaims any and all liability for any losses that may arise from this functionality being enabled. Customer is responsible to determine if this functionality should remain enabled or disable it	All data is securely wiped from the Garrison node at the end of a session and cannot be accessed by anyone except the Authorised User that is currently on the node	Data Processor	Data Controller	Garrison Affiliates and AWS	The transfer will move from where Authorised User is physically located to where Authorised User is browsing from
Any files downloaded by Authorised Users using Garrison ULTRA®	Authorised Users	For the provision of Garrison ULTRA® and in particular for enabling download of files from the Garrison ULTRA® isolated environment	Files downloaded during or across Authorised User Browsing sessions. Where file downloads to the local device are enabled, files are transferred then stored and encrypted in AWS	File downloads are stored for 2 (two) days before being wiped	Data Processor	Data Controller	Garrison Affiliates and AWS	Customer must choose the home region of their choice at the start of onboarding The transfer will move from where Authorised User is browsing from, through the elected home region and then onward to where Authorised User physically is

Type of Personal Data	Category of Data Subject	Purpose	Nature	Duration	Garrison	Customer	Sub-Processors?	Transferred outside Customer home region?
Any files emailed by Authorised Users using Garrison ULTRA®	Authorised Users	For the provision of Garrison ULTRA® and in particular for enabling email transfer of files from the Garrison ULTRA® isolated environment	Files downloaded during or across Authorised User Browsing sessions When a file is sent via email the file is relayed through AWS and then forwarded to Authorised User's email address of choice This functionality is enabled by default Files emailed in this way may be malicious and the Garrison ULTRA® Service does not enable any security measures to prevent this. Garrison expressly disclaims any and all liability for any losses that may arise from this functionality being enabled Customer is responsible to determine if this functionality should remain enabled or disable it and where enabled to ensure such email transfer occurs in accordance with Customer corporate policies and Garrison's AUP	Email transfers are forwarded and not stored	Data Processor	Data Controller	Garrison Affiliates and AWS	Customer must choose the home region of their choice at the start of onboarding The transfer will move from where Authorised User is browsing from, through the elected home region and then onward to where the elected email recipient physically is
Logs of Authorised User actions against service APIs Data includes the Authorised User username, the time and the action name For example, if an Authorised User	Authorised Users	For provision and management of Garrison ULTRA® by Garrison	Data stored and encrypted by AWS	For 36 (thirty-six) months from when logs were generated	Data Processor	Data Controller	Garrison Affiliates and AWS	Customer must choose the home region of their choice at the start of onboarding If the elected home region is not where Authorised User is located, this will necessitate a transfer to a third country

Type of Personal Data	Category of Data Subject	Purpose	Nature	Duration	Garrison	Customer	Sub-Processors?	Transferred outside Customer home region?
transfers a file to their local machine, this action will be logged (but without further details such as the filename)								
Logs of Authorised User actions in Garrison ULTRA® web app Data includes the Authorised User username, the time, and the action name For example, if an Authorised User pastes content from their local machine, this action will be logged (but without further details such as the content)	Authorised Users	For provision and management of Garrison ULTRA® by Garrison	Data stored and encrypted by AWS	For 36 (thirty-six) months from when logs were generated	Data Processor	Data Controller	Garrison Affiliates and AWS	Customer must choose the home region of their choice at the start of onboarding If the elected home region is not where Authorised User is located, this will necessitate a transfer to a third country
Logs of Authorised User actions in Garrison ULTRA® against service APIs and in the Garrison ULTRA® web app	Authorised Users	For provision and management of Garrison ULTRA® by Garrison	Download of anonymised data stored and encrypted by AWS onto Garrison corporate infrastructure and analysis of such data	Anonymised data will be kept indefinitely	Data Processor	Data Controller	Garrison Affiliates and AWS	No transfer

APPENDIX B – DATA AND SYSTEM SECURITY POLICY FOR THE GARRISON ULTRA® SERVICE

Domain	Practices
Organisation of Information Security	**Security Ownership**: Garrison has appointed one or more security officers responsible for coordinating and monitoring the security rules and procedures **Security Roles and Responsibilities**: Garrison personnel with access to Personal Data are subject to confidentiality obligations **Risk Management Program**: Garrison performed a risk assessment before launching Garrison ULTRA® Garrison retains its security documents pursuant to its retention requirements after they are no longer in effect
Asset Management	**Asset Inventory**: Garrison maintains an inventory of all assets used to provide the Garrison ULTRA® service including those which are used to hold or process Personal Data. The inventory includes details of ownership, business criticality, service-level expectations, and version history
Human Resources Security	**Security Training**: Garrison informs its personnel about relevant security procedures. Garrison also informs its personnel of possible consequences of breaching the security rules and procedures
Physical and Environmental Security	**Physical Access to Facilities**: Garrison limits access to facilities where information systems that process Personal Data or Professional Services Data are located to identified authorised individuals **Protection from Disruptions**: Garrison uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference **Component Disposal**: Garrison uses industry standard processes to delete Personal Data when it is no longer needed
Communications and Operations Management	**Operational Policy**: Garrison maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Personal Data **Data Recovery Procedures**: - Garrison takes backups of the Garrison ULTRA® infrastructure daily - Garrison maintains documented procedures on how to restore data from backups **Malicious Software**: Garrison has anti-malware controls to help avoid malicious software gaining unauthorised access to Personal Data **Data Beyond Boundaries**: Garrison encrypts Personal Data that is transmitted over public networks **Event Logging**: Garrison logs access and use of information systems containing Personal Data

Access Control	**Access Policy**: Garrison restricts access to Personal Data to identified authorised personnel only **Access Authorisation**: - Garrison maintains and updates records of personnel authorised to access systems containing Personal Data - Garrison deactivates authentication credentials that have not been used for a period of time not to exceed six months - Garrison identifies those personnel who may grant, alter, or cancel authorised access to data and resources - Garrison ensures that where more than one individual has access to systems containing Personal Data, the individuals have separate identifiers/log-ins **Least Privilege**: Garrison restricts access to Personal Data to only those individuals who require such access to perform their job function **Authentication**: - Garrison uses industry standard practices to identify and authenticate users who attempt to access information systems - Where authentication mechanisms are based on passwords, Garrison requires the password to be at least fourteen characters long - Garrison ensures that de-activated or expired identifiers are not granted to other individuals - Garrison maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed - Garrison uses industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage
	Network Design: Garrison has controls to avoid individuals assuming access rights they have not been assigned to gain access to Personal Data they are not authorised to access
Information Security Incident Management	**Incident Response Process**: - Garrison maintains records of security events and incidents with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported - For each security incident that concerns Personal Data, Garrison will notify Data Controllers without undue delay **Service Monitoring**: Security logs are retained and are reviewed quarterly
Business Continuity Management	- Garrison maintains emergency and contingency plans for the facilities in which Garrison information systems that process Personal Data are located - Garrison's redundant storage and its procedures for recovering data are designed to attempt to reconstruct Personal Data in its original or last replicated state from before the time it was lost or destroyed