CYBERGYM Data Processing Notice

In connection with an actual or explored business transaction or relationship, CYBERGYM GLOBAL PTY Limited ("CYBERGYM", "We" or "Us"), may receive, collect, discern, analyze, combine, create, store, use or otherwise manipulate (collectively, "Process"), either alone or with the assistance of others such as advisors. sub-contractors and service providers, various information pertaining to customers and prospects (collectively, "Clients"), as well as share, disclose or allow access to such information, or to parts thereof (collectively, "Client Data"), to certain third parties both in and outside the Commonwealth of Australia.

The purpose of this Data Processing Notice (the "Notice" or "this Document") is to notify CYBERGYM's Clients of:

- what Client Data we will be accessing or storing;
- who will have access to the Client Data;
- where will the Client Data be stored; and
- how will the Client Data be protected, including by any service providers who will have access to the facilities owned or operated by CYBERYGYM.

This Notice is intended to supplement the provisions of any other binding agreement or legal undertaking entered between CYBERGYM or any other company within the CyberGym group (including CyberGym Control Ltd), and the pertinent Client, whether in general or in connection with a specific engagement or action, including the terms of any commercial transaction, Non-Disclosure Agreement ('NDA' or 'MNDA'), Personal Data Processing Addendum ('DPA') etc.

What Client Data we will be accessing or storing?

The types and categories of Client Data we will be Processing, as well as their categorization in terms of sensitivity (as furthest explained below) are as follows:

Type of engagement/ service	**Processed Client Data**	**Sensitivity**
General (including pre-contractual stages)	**Marketing, Sales and Customer Relations Information-** These include contact details of the Client's sales and management team (business address as well as email, phone, fax etc.), their title and role within the Client's organization, links to business webpage(s) or business-oriented social networks (e.g., LinkedIn), summaries and transcriptions of meetings and calls, copies of correspondence as well as feedbacks and qualitative and quantitative data past, current or prospective future engagements.	Protected*

Type of engagement/ service	Processed Client Data	Sensitivity
Negotiated or entered business engagements (all)	• **Compliance & Risk Evaluation** – We may be required by applicable laws and regulations, or by risk management standards and policies which we follow, to conduct certain pre-contractual examinations such as queries against Sanctions lists and public registers as well as examination and evaluation of other publicly available information. • **Contractual Data** – to facilitate the business engagement We will be processing information identifying the legal entity with which we engage (the entity's name and officially registered business address, ACN or other official identifier), as well as the Client's signatories and legal representatives for the purposes of the pertinent engagement, the terms of the specific engagement (including any supplementary, ancillary or additional legal instruments, annexes or appendices) and any applicable framework or governing agreement or rules. Additionally, we will record and Process information and evidence about the contractual performance, and any claims made or remedies sought by either party. • **Payment and Financial Data –** We will be Processing payment and financial data such as the contractual payment terms and amounts, details of payees' bank account(s), details of current and past payments made and received, whether to the Client or any related third party, details of any guarantees received or provided, etc.	**Protected**
Training Services	**Limited Trainees' Data** - We will collect the names of the Trainees (first name only unless certifications of completing the trainings is provided in which case We will need full names), and, in online-based trainings also their business emails for invitation and login purposes.	**Protected**

Type of engagement/ service	Processed Client Data	Sensitivity
Penetration Testing and Vulnerability Assessment Services	**Client's Cyber Environment(s) information and Vulnerabilities -** We will collect, discern, create and Process, in preparation for and during or otherwise as a result of or in connection with the services we shall be providing, information pertaining to components, topology, set-up, configuration, credentials and vulnerabilities of, as well as threats to and cyber risk associated with, the Client's Information Technology (and, as the case may be, Operational Technology) cyber environments. *(exact scope of Processed Client Data is dependent the SOW and on the nature and set-up of the pertinent environments)*	**Sensitive**

Risk-Based Data Classification

Our Processing of Client Data is guided by a risk-based approach to the implementation of appropriate technical and organizational measures to ensure the integrity, security, confidentiality and privacy of the Client Data based on its classification into one of the following levels of sensitivity:

- **Protected** – in general we treat all Client Data as protected, taking reasonable and customary measures to protect its integrity, security, confidentiality and privacy. The only exception to the aforesaid, is generally available **Public** data which does not pertain to identified or identifiable individual (i.e. does not qualify as "Personal Data" under applicable privacy laws and regulations), and further provided that such data has not been afforded confidential status under any applicable contractual undertaking (such as an NDA or the terms and condition of the commercial engagement with the Client).

- **Sensitive** – information which would, if subject of any unauthorized access or modification, be reasonably likely to cause material loss or damage to the Client or to other third parties (such as technical information or reports which would be reasonably likely to allow a malicious actor to compromise the confidentiality, integrity or availability of the Client's IT environment) is categorized as Sensitive and is afforded, accordingly, stricter protection than other Protected Client Data, including more stringent limitations and additional controls on its use, storage, transfer and sharing or other types of Processing.

Who will have access to Client Data?

Other than our own employees and managers, who will be also provided with access to Client Data solely on a "need to know" basis, CYBERGYM shall allow access to Client Data, only too the following entities:

- **Service Providers of the IT systems we use** – CYBERGYM manages and Processes all data, including Client Data, using cloud-based renowned third-party solutions and systems (such as Salesforce and Microsoft SharePoint), as further detailed in the "Storage and Protection of Client Data" section below. Thus, the aforesaid Service Providers have access to the Client Data stored therein.

- **Our professional Advisors and Consultants** – As part of our ordinary conduct of business, as well as in order to enforce our rights, we are being assisted by professional advisors and consultants such as CPA and lawyers and will be providing them with access to relevant Client Data, and in particular to Contractual, Payment and Financial Data.

- **Sub-contractors** – in certain circumstances, and subject to any conditions and restrictions imposed in our contract with the pertinent Client, we might be assisted by professional third-party Sub-contractors to provide our servicers or to fulfill certain of our contractual duties.

- **Auditors** – our financial auditors will be granted with access to Client Data, and in particular to contractual and financial data, to the extent required for the discharge of their duties under applicable financial auditing standards.

- **Regulators, Investigative Bodies and other Legal Authorities** – CYBERGYM might be required to provide access to Client Data under applicable Australian state, territory or commonwealth laws and regulations .

- **Special Restrictions on allowing Access within CYBERGYM'S control group**

Notwithstanding the aforesaid, certain specific restrictions have been imposed by the authorized authority in connection with allowing access to Client Data to CYBERGYM's sole shareholder - CyberGym Control Ltd. (an Israeli private company) ("CG Israel") as well to Israel Electric Corporation Ltd. (an Israeli governmental company, which is a shareholder wth a controlling interest in CyberGym Control Ltd.) ("IEC") and entities in their control group (collectively, the "Restricted Entities").

Pursuant to the aforesaid restrictions, directors, executive managers and employees (and their agents and representative) of any of the Restricted Entities may not be allowed access or disclosure to, or use of Client Data except where any of the following Exceptions apply:

Exception	Possible Application
The access is required by CYBERGYM's employees for the purpose of delivering its business services	Leveraging the uniquely acquired experience and skillset of Israeli cyber experts employed by CG Israel (such as its offensive cyber team members and cyber defense trainers) for the provision of services; being assisted by the legal and financial teams located at the group's headquarters in Israel to facilitate the relevant aspects of the contractual engagement

Exception	Possible Application
The access is required to discharge duties as a director or executive manager under Australian law; or	Providing CG Israel's representative on CYBERGYM's Board of Directors with access to technical, commercial, legal and other related Client Data to the extent required to allow for effective discharge of the Director's duties of care and fiduciary duties in supervising and auditing CYBERGYM's strategy, activities and management
Access is required to comply with any Australian Law	Granting CG Israel's and IEC's personnel with access to certain Client Data as might be required for them to demonstrate compliance with the access restrictions imposed by an Australian regulator

Where will the Client Data be stored and how will it be secured?

Other than temporarily as might be required for viewing and Processing Client Data on endpoint IT systems (see below), all Client Data is stored and Processed remotely in the cloud in the following system(s) 0f the pertinent solution provider with the data on such systems being secured as detailed opposite their name:

System/ Solution Used	Categories of Client Data	Applied Security Measures (as published by provider)
Salesforce	Marketing, Sales & CRM	https://www.salesforce.com/content/dam/web/en_us/www/documents/legal/Privacy/dpia-and-salesforce-services.pdf
Lightyear	Financial Data (Invoicing)	https://acornitsolutions.com/privacy-policy/
XERO	Financial Data (Bookkeeping and other)	https://www.xero.com/au/security/
SharePoint	Contractual Data, Compliance & Risk Evaluation Data	https://docs.microsoft.com/en-us/sharepoint/safeguarding-your-data
Microsoft Azure	PT & Vulnerability Testing related data and work in progress	https://docs.microsoft.com/en-us/azure/security/fundamentals/overview
Microsoft 365	email	https://docs.microsoft.com/en-us/microsoft-365/security/?view=o365-worldwide

Securing Endpoints and Data in Transit

All endpoints are installed with regularly updated operating system, anti-virus and firewall with all Protected and Sensitive data encrypted at rest and in transit.

Additional security measures and controls we implement to protect the integrity, security, confidentiality and privacy of both Sensitive and Protected Client Data include:

- Logical access control and Data Loss Prevention tool
- Use of strong authentication for access to cloud-based systems and resources

- Use of Security Information and Event Management (SIEM) tool
- Periodic vulnerability assessments
- Procedures and means for secure storage, handling and destruction of media
- Physical protection measures and access control to facilities
- Internal policies and procedures and employee trainings
- Sub-contractor vetting and contractual imposition of security requirements

Further technical and organizational security measures (such as work from client premises, pseudo-anonymization, use of newly purchased or installed Endpoints etc.) might be implemented in coordination with the Client to protect the confidentiality of Sensitive Client Data, and in particular Client's Cyber Environment(s) information and Vulnerabilities.

Notification about Material Operational Changes

We shall inform our clients within 30 days of:

- any material changes occurring to the operational management or day-to-day control of our facilities in Australia; and
- any changes of service providers who provide services relating to the secured parts of the the facilities in Australia owned or operated by the us (including security guards, cleaners and IT contractors).