DATA PROTECTION POLICY – GYM NATION LONDON BRIDGE LIMITED

INTRODUCTION

This Data Protection Policy sets out how **GYM NATION LONDON BRIDGE LIMITED (‘**the Company’) handles the Personal Data of our customers, suppliers, employees, workers and other third parties.

This Data Protection Policy applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other Data Subject. It applies to all Company Personnel (” you”, “your”) including Andy Parsons. You must read, understand and comply with this Data Protection Policy when Processing Personal Data on our behalf and attend training on its requirements. This Data Protection Policy sets out what we expect from you in order for the Company to comply with applicable law. Your compliance with this Data Protection Policy is mandatory. Any breach of this Data Protection Policy or other related policies may result in disciplinary action.

This Data Protection Policy (together with related policies) is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from the Company.

SCOPE

Andy Parsons is responsible for overseeing this Data Protection Policy and, as applicable, developing Related Policies and Privacy Guidelines.

Please contact the above named with any questions about the operation of this Data Protection Policy or the GDPR or if you have any concerns that this Data Protection Policy is not being or has not been followed.

PERSONAL DATA PROTECTION PRINCIPLES

We adhere to the principles relating to Processing of Personal Data set out in the GDPR which require Personal Data to be:

(a) Processed lawfully, fairly and in a transparent manner

(b) Collected only for specified, explicit and legitimate purposes

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed

(d) Accurate and where necessary kept up to date

(e) Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed

(f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage

(g) Not transferred to another country without appropriate safeguards being in place

(h) Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data.

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above as set out below;

i. Personal data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. You may only collect, process and share Personal Data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

The GDPR allows Processing for specific purposes, some of which are where the Data Subject has given his or her Consent; where the Processing is necessary for the performance of a contract with the Data Subject; to meet our legal compliance obligations; to protect the Data Subject's vital interests; and to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices or you must identify and document the legal ground being relied on for each Processing activity.

ii. A Data Controller must only process Personal Data on the basis of one or more of the lawful bases set out in the GDPR, which include Consent.

A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters. Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

iii. The GDPR requires Data Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them. Whenever we collect Personal Data directly from Data Subjects, including for HR or employment purposes, we must provide the Data Subject with all the information required by the GDPR including the identity of the Data Controller and DPO, how and why we will use, Process, disclose, protect and retain that Personal Data through a Privacy Notice which must be presented when the Data Subject first provides the Personal Data. When Personal Data is collected indirectly (for example, from a third party or publically available source), you must provide the Data Subject with all the information required by the GDPR as soon as possible after collecting/receiving the data. You must also check that the Personal Data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

iv. Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed. You may only Process Personal Data when performing your job duties requires it. You cannot Process Personal Data for any reason unrelated to your job duties. Do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes. You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Company's data retention guidelines.

v. Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

vi. Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed. You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

Data relating to candidates who have applied to work for or be engaged in any way with or for the Company and been unsuccessful will be kept for a period of 6 months after the date they submitted their application, after which the information will be confidentially destroyed. Data relating to actively employed/engaged personnel will be reviewed annually to ensure out of date or irrelevant data is removed/updated. Data relating to ex-employees/workers will be kept for a period of 6 years after they have left the Company, after which the majority of data will be confidentially destroyed except where required by law.

vii. Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes. You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have Consented where necessary.

You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all the Company's applicable records retention schedules and policies. This includes requiring third parties to delete such data where applicable. You will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice or Fair Processing Notice.

viii. Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage. You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

ix. Everyone who works for, or on behalf of, the Company has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy.

Andy Parsons is responsible for reviewing this policy and updating senior management on the Company's data protection responsibilities and any risks in relation to the processing of data. You should direct any questions in relation to this policy or data protection to this person.

<u>Specifics</u>

You should only access personal data covered by this policy if you need it for the work you do for, or on behalf of the Company and only if you are authorised to do so. You should only use the data for the specified lawful purpose for which it was obtained.

You should not share personal data informally.

You should keep personal data secure and not share it with unauthorised people.

You should regularly review and update personal data which you have to deal with for work. This includes telling us if your own contact details change.

You should not make unnecessary copies of personal data and should keep and dispose of any copies securely.

You should use strong passwords, never share them and change them regularly.

You should lock your computer screens when not at your desk.

Consider processing personal data in a way so that you can't tell from looking at it which person it relates to. You would need additional information (a key or code) kept separately (and securely) to decode it. (Known as 'pseudonymisation'.)

Do not save personal data to your own personal computers or other devices.

Personal data should never be transferred outside the European Economic Area except in compliance with the law and authorisation of the Company.

You should lock drawers and filing cabinets. Do not leave paper with personal data lying about.

You should not take personal data away from Company's premises without authorisation from your manager.

Personal data should be shredded and disposed of securely when you have finished with it.

Any deliberate or negligent breach of this policy by you may result in disciplinary action being taken against you in accordance with our disciplinary procedure.

It is a criminal offence to conceal or destroy personal data which is part of a subject access request (see below). This conduct would also amount to gross misconduct under our disciplinary procedure, which could result in your dismissal.

REPORTING A PERSONAL DATA BREACH

The GDPR requires Data Controllers to notify any Personal Data Breach to the applicable regulator and, in certain instances, the Data Subject. We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the person designated as the key point of contact for Personal Data Breaches (Andy Parsons) and follow the procedure for breaches. You should preserve all evidence relating to the potential Personal Data Breach.

TRANSFER LIMITATION

We do not transfer data outside of the EEA.

DATA SUBJECT'S RIGHTS AND REQUESTS

Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

(a) withdraw Consent to Processing at any time;

(b) receive certain information about the Data Controller's Processing activities;

(c) request access to their Personal Data that we hold;

(d) prevent our use of their Personal Data for direct marketing purposes;

(e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;

(f) restrict Processing in specific circumstances;

(g) challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;

(h) request a copy of an agreement under which Personal Data is transferred outside of the EEA;

(i) object to decisions based solely on Automated Processing, including profiling (ADM);

(j) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

(k) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

(l) make a complaint to the supervisory authority; and

(m) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format.

You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

You must immediately forward any Data Subject request you receive to Andy Parsons and comply with the Company's Data Subject response process.

ACCOUNTABILITY

The Data Controller must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The Data Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

The Company must have adequate resources and controls in place to ensure and to document GDPR compliance including:

(a) appointing an executive accountable for data privacy (Andy Parsons);

(b) integrating data protection into internal documents including this Data Protection Policy, Related Policies, Privacy Guidelines, Privacy Notices or Fair Processing Notices;

(c) regularly training any Company Personnel on the GDPR, this Data Protection Policy, Related Policies and Privacy Guidelines and data protection matters including, for example, Data Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches. The Company must maintain a record of training attendance by Company Personnel; and

(d) regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

RECORD KEEPING

The GDPR requires us to keep full and accurate records of all our data Processing activities. You must keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents.

These records should include, at a minimum, the name and contact details of the Data Controller and the DPO, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place. In order to create such records, data maps should be created which should include the detail set out above together with appropriate data flows.

TRAINING AND AUDIT

We are required to ensure all Company Personnel have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance. You must undergo all mandatory data privacy related training and ensure your team undergo similar mandatory training.

You must regularly review all the systems and processes under your control to ensure they comply with this Data Protection Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

AUTOMATED PROCESSING (INCLUDING PROFILING) AND AUTOMATED DECISION-MAKING

We do not carry out automated processing.

DIRECT MARKETING

We are subject to certain rules and privacy laws when marketing to our customers.

For example, a Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

A Data Subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

SHARING PERSONAL DATA

Generally we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

You may only share the Personal Data we hold with another employee, agent or representative of our group (which includes our subsidiaries and our ultimate holding company along with its subsidiaries) if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

You may only share the Personal Data we hold with third parties, such as our service providers if:

(a) they have a need to know the information for the purposes of providing the contracted services;

(b) sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;

(c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;

(d) the transfer complies with any applicable cross border transfer restrictions; and

(e) a fully executed written contract that contains GDPR approved third party clauses has been obtained.

CHANGES TO THIS DATA PROTECTION POLICY

We reserve the right to change this Data Protection policy at any time without notice to you so please check back regularly to obtain the latest copy of this Data Protection Policy. This Data Protection Policy does not override any applicable national data privacy laws and regulations in countries where the Company operates.

DEFINITIONS

Automated Decision-Making (ADM): when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

Automated Processing: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

Company Personnel: all employees, workers, contractors, agency workers, consultants, directors, members and others.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

Data Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. We are the Data Controller of all Personal Data relating to our Company Personnel and Personal Data used in our business for our own commercial purposes.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Protection Officer (DPO): the person required to be appointed in specific circumstances under the GDPR. Where a mandatory DPO has not been appointed, this term where used below means a data protection manager or other voluntary appointment of a DPO or refers to the Company data privacy team with responsibility for data protection compliance – Andy Parsons.

EEA: the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

General Data Protection Regulation (GDPR): the General Data Protection Regulation ((EU) 2016/679). Personal Data is subject to the legal safeguards specified in the GDPR.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Sensitive Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy Notice: a separate notice setting out information that may be provided to Data Subjects when the Company collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one-time privacy statements covering Processing related to a specific purpose.

Processing or Process: 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 transmitting or transferring Personal Data to third parties.

Sensitive Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions including drug screening, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.