Hypertune Ltd
Data Processing Addendum

This Data Processing Addendum including its Annexes ("DPA") forms part of the Terms and Conditions or other written agreement between Hypertune and Customer to reflect the Parties' agreement with regard to the Processing of Personal Data. Hypertune takes the security of Personal Data seriously and relies on the General Data Protection Regulation which Hypertune regard as the gold standard for data protection.

This DPA sets out the additional terms, requirements and conditions on which Hypertune shall process Personal Data when providing services under the Terms and Conditions. This DPA contains the mandatory clauses required by Article 28(3) of the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (UK GDPR) for contracts between controllers and processors and the General Data Protection Regulation ((EU) 2016/679).

AGREED TERMS

1. Definitions and interpretation

The following definitions and rules of interpretation apply in this DPA.

1.1 Definitions:

1 **Business Purposes**: the services to be provided by Hypertune to the Customer as described in the Terms and Conditions and any other purpose specifically identified in Annex A.

2 **Commissioner:** the Information Commissioner (see Article 4(A3), UK GDPR and section 114, DPA 2018).

3 **Controller, Processor, Data Subject, Personal Data, Personal Data Breach and Processing**: have the meanings given to them in the Data Protection Legislation.

4 **Controller:** has the meaning given to it in section 6, DPA 2018.

5 **Data Protection Legislation:** To the extent the UK GDPR applies, the law of the United Kingdom or of a part of the United Kingdom which relates to the protection of Personal Data and to the extent the EU GDPR applies, the law of the European Union or any member state of the European Union to which the Customer or Hypertune is subject which relates to the protection of Personal Data.

6 **Data Subject**: the identified or identifiable living individual to whom the Personal Data relates.

7 **EU GDPR:** the General Data Protection Regulation ((EU) 2016/679).

8 **EEA:** the European Economic Area.

9 **Personal Data**: means any information relating to an identified or identifiable living individual that is processed by Hypertune on behalf of the Customer as a result of, or in connection with, the provision of the services under the Terms and Conditions; an identifiable living individual is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

10 **Processing, processes, processed, process**: any activity that involves the use of the Personal Data. It includes, but is not limited to, any operation or set of operations which is performed on the Personal Data or on sets of the Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring the Personal Data to third parties.

11 **Personal Data Breach**: a breach of security leading to the accidental, unauthorised or unlawful destruction, loss, alteration, disclosure of, or access to, the Personal Data.

12 **Processor**: a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller.

13 **Records**: has the meaning given to it in Clause 12.

14 **Standard Contractual Clauses (SCC)**: the European Commission's Standard Contractual Clauses for the transfer of Personal Data from the European Union to processors established in third countries (controller-to-processor transfers), as set out in the Annex to Commission Decision 2010/87/EU as adapted

for the UK, a completed copy of which comprises Annex C or such alternative clauses as may be approved by the European Commission or by the UK from time to time.

15 **Term**: this DPA's term as defined in Clause 10.

16 **UK GDPR:** has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the DPA 2018.

1.2 This DPA is subject to the terms of the Terms and Conditions and is incorporated into the Terms and Conditions. Interpretations and defined terms set forth in the Terms and Conditions apply to the interpretation of this DPA.

1.3 The Annexes form part of this DPA and shall have effect as if set out in full in the body of this DPA. Any reference to this DPA includes the Annexes.

1.4 In the case of conflict or ambiguity between any of the provisions of this DPA and any executed SCC the provisions of the executed SCC will prevail.

2. Personal data types and processing purposes

2.1 The Customer and Hypertune agree and acknowledge that for the purpose of the Data Protection Legislation:

(a) the Customer is the Controller and Hypertune is the Processor.

(b) the Customer retains control of the Personal Data and remains responsible for its compliance obligations under the applicable Data Protection Legislation, including but not limited to providing any required notices and obtaining any required consents, and for the written Processing instructions it gives to Hypertune.

(c) Annex A describes the subject matter, duration, nature and purpose of the Processing and the Personal Data categories and Data Subject types in respect of which Hypertune may process the Personal Data to fulfil the Business Purposes.

3. Hypertune's obligations

3.1 Hypertune shall only process the Personal Data to the extent, and in such a manner as is necessary for the Business Purposes in accordance with the Customer's written instructions. Hypertune shall not process the Personal Data for any other purpose or in a way that does not comply with this DPA or the Data Protection Legislation. Hypertune must promptly notify the Customer if in its opinion the Customer's instructions do not comply with the Data Protection Legislation.

3.2 The Customer acknowledges that as part of the provision of the services, Hypertune may collect, disclose, publish, share and otherwise use fully anonymized, de-identified and de-identifiable data, including statistical data, analytics, trends and other aggregated data derived from Personal Data processed by Hypertune as part of the provision of the services, all as required for Hypertune's legitimate purposes, such as to provide, maintain, operate and improve the services and for research purposes. The Customer agrees and acknowledges that such Processing activities (including the anonymization and de-identification of Personal Data) will not be considered as performed outside the scope of the instructions provided by the Customer hereunder. Hypertune agrees not to use said anonymized or de-identified data in a form that identifies the Customer or any Data Subject.

3.3 Notwithstanding clause 3.2 Hypertune shall comply with any Customer written instructions requiring Hypertune to amend, transfer, delete or otherwise process the Personal Data or to stop, mitigate or remedy any unauthorised Processing.

3.4 Hypertune shall maintain the confidentiality of the Personal Data and shall not disclose the Personal Data to third parties unless the Customer or this DPA specifically authorises the disclosure, or as required by domestic law, court or regulator including the Commissioner. If a domestic law, court or regulator including the Commissioner requires Hypertune to process or disclose the Personal Data to a third party, Hypertune must first inform the Customer of such legal or regulatory requirement and give the Customer an opportunity to object or challenge the requirement, unless the domestic law prohibits the giving of such notice.

3.5 Hypertune shall reasonably assist the Customer with meeting the Customer's compliance obligations under the Data Protection Legislation, taking into account the nature of Hypertune's Processing and the information available to Hypertune including in relation to Data Subject rights, data protection impact assessments and

reporting to and consulting with the Commissioner or other relevant regulator under the Data Protection Legislation.

3.6 Hypertune shall promptly notify the Customer of any changes to the Data Protection Legislation that may reasonably be interpreted as adversely affecting Hypertune's performance of the Terms and Conditions or this DPA.

4. Hypertune's employees

4.1 Hypertune shall ensure that all of its employees:

(a) are informed of the confidential nature of the Personal Data and are bound by confidentiality obligations and use restrictions in respect of the Personal Data;

(b) are aware both of Hypertune's duties and their personal duties and obligations under the Data Protection Legislation and this DPA.

5. Security

5.1 Hypertune shall implement appropriate technical and organisational measures against unauthorised or unlawful Processing, access, copying, modification, reproduction, display or distribution of the Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of Personal Data including but not limited to the security measures set out in Annex B.

5.2 Hypertune shall implement such measures to ensure a level of security appropriate to the risk involved including as appropriate:

(a) the pseudonymisation and encryption of Personal Data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;

(c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and

(d) a process for regularly testing, assessing and evaluating the effectiveness of the security measures.

6. Personal Data Breach

6.1 Hypertune shall without undue delay notify the Customer if it becomes aware of:

(a) the loss, unintended destruction or damage, corruption, or unusability of part or all of the Personal Data. Hypertune shall restore such Personal Data at its own expense as soon as possible.

(b) any accidental, unauthorised or unlawful Processing of the Personal Data; or

(c) any Personal Data Breach.

6.2 Where Hypertune becomes aware of (a), (b) and/or (c) above it shall without undue delay provide the Customer with the following information:

(a) description of the nature of (a), (b) and/or (c), including the categories of in-scope Personal Data and approximate number of both Data Subjects and the Personal Data records concerned;

(b) the likely consequences; and

(c) a description of the measures taken or proposed to be taken to address (a), (b) and/or (c), including measures to mitigate its possible adverse effects.

6.3 Immediately following any accidental, unauthorised or unlawful Personal Data Processing or Personal Data Breach, the parties shall co-ordinate with each other to investigate the matter. Further, Hypertune shall reasonably co-operate with the Customer in the Customer's handling of the matter, including but not limited to:

(a) assisting with any investigation;

(b) where necessary providing the Customer with physical access to any facilities and operations affected;

(c) making available all relevant records, logs, files, data reporting and other materials required to comply with all Data Protection Legislation or as otherwise reasonably required by the Customer; and

(d) taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Personal Data Breach or accidental, unauthorised or unlawful Personal Data Processing.

6.4 Hypertune shall not inform any third party of any accidental, unauthorised or unlawful Processing of all or part of the Personal Data and/or a Personal Data Breach without first obtaining the Customer's written consent, except when required to do so by domestic law.

7. Cross-border transfers of personal data

7.1 Hypertune shall process the Personal Data outside the UK/EEA under the following conditions: (a) Hypertune processes the Personal Data in a territory which is subject to adequacy regulations or decisions under the Data Protection Legislation in that the territory provides adequate protection for the privacy rights of individuals; or (b) Hypertune participates in a valid cross-border transfer mechanism under the Data Protection Legislation to ensure an adequate level of protection with respect to the privacy rights of individuals as required by Data Protection Legislation in Article 46 of the UK GDPR and EU GDPR.

8. Sub-processor(s)

8.1 Hypertune has the Customer’s general authorisation for the engagement of sub-processor(s) from an agreed list (Refer to Annex A). Hypertune shall inform the Customer in writing of any intended changes to that list through the addition or replacement of sub-processors at least 20 working days in advance thereby giving the Customer sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). Hypertune shall provide the Customer with the information necessary to enable the Customer to exercise its right to object.

8.2 Where Hypertune engages a sub-processor to carry out specific Processing activities it shall do so by way of a written contract that provides for in substance the same data protection obligations as those binding Hypertune under these clauses including in terms of third-party beneficiary rights for data subjects.

8.3 Hypertune shall remain fully responsible to the Customer for the performance of the sub-processor’s obligations under its contract with Hypertune. Hypertune shall notify the Customer of any failure by the sub-processor to fulfil its obligations under that contract.

8.4 Hypertune shall agree a third-party beneficiary clause with the sub-processor whereby in the event Hypertune has factually disappeared, ceased to exist in law or has become insolvent the Customer shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the Personal Data.

9. Complaints, data subject requests and third-party rights

9.1 Hypertune shall take such technical and organisational measures as may be appropriate and promptly provide such information to the Customer as the Customer may reasonably require to enable the Customer to comply with:

(a) the rights of Data Subjects under the Data Protection Legislation, including subject access rights, the rights to rectify, port and erase Personal data, object to the Processing and automated Processing of Personal Data, and restrict the Processing of Personal Data; and

(b) information or assessment notices served on the Customer by the Commissioner or other relevant regulator under the Data Protection Legislation.

9.2 Hypertune shall notify the Customer in writing within 3 business days if it receives any complaint, notice or communication that relates directly or indirectly to the Processing of the Personal Data or to either party's compliance with the Data Protection Legislation.

9.3 Hypertune shall notify the Customer within 3 business days if it receives a request from a Data Subject for access to their Personal Data or to exercise any of their other rights under the Data Protection Legislation.

9.4 Hypertune shall give the Customer reasonable co-operation and assistance in responding to any complaint, notice, communication or Data Subject request.

10. Term and termination

10.1 This DPA will remain in full force and effect so long as the Terms and Conditions remains in effect.

10.2 Any provision of this DPA that expressly or by implication should come into or continue in force on or after termination of the Terms and Conditions in order to protect the Personal Data will remain in full force and effect.

10.3 If a change in any Data Protection Legislation prevents either party from fulfilling all or part of its Terms and Conditions obligations, the parties may agree to suspend the Processing of the Personal Data until that Processing complies with the new requirements. If the parties are unable to bring the Personal Data Processing into compliance with the Data Protection Legislation 30 business days, either party may terminate the Terms and Conditions on written notice to the other party.

11. Data return and destruction

11.1 At the Customer's request Hypertune shall give the Customer or a third party nominated in writing by the Customer a copy of or access to all or part of the Personal Data in its possession or control in the format and on the media reasonably specified by the Customer.

11.2 On termination of the Terms and Conditions for any reason or expiry of its term Hypertune shall securely delete or destroy or, if directed in writing by the Customer, return and not retain all or any of the Personal Data related to this DPA in its possession or control unless any law, regulation, or government or regulatory body requires Hypertune to retain any documents or materials or Personal Data that Hypertune would otherwise be required to return or destroy.

12. Records

12.1 Hypertune shall keep accurate written records regarding any Processing of the Personal Data, including but not limited to, the access, control and security of the Personal Data, approved subcontractors, the Processing purposes, categories of Processing, any transfers of Personal Data to a third country and related safeguards, and a general description of the technical and organisational security measures referred to in 5.1 (**Records**).

12.2 Hypertune shall ensure that the Records are sufficient to enable the Customer to verify Hypertune's compliance with its obligations under this DPA and Hypertune shall provide the Customer with copies of the Records upon request.

13. Audit

13.1 Hypertune shall permit the Customer and its third-party representatives to audit Hypertune's compliance with its DPA obligations, on at least 30 working days' notice, during the Term. Any audit for the purpose of compliance with DPA obligations shall be limited to one audit per calendar year.

13.2 Hypertune shall give the Customer and its third-party representatives all necessary assistance to conduct such audits. The assistance may include:

(a) remote electronic access to, and copies of the Records and any other information held at the Hypertune's premises or on systems storing the Personal Data; and

(b) reasonable inspection of relevant Records and relevant infrastructure, electronic data or systems, facilities, equipment or application software used to store, process the Personal Data.

14. Warranties

14.1 Hypertune warrants and represents that:

(a) it and anyone operating on its behalf shall process the Personal Data in compliance with the Data Protection Legislation and other laws, enactments, regulations, orders, standards and other similar instruments;

(b) it has no reason to believe that the Data Protection Legislation prevents it from providing any of the Terms and Conditions contracted services; and

(c) considering the current technology environment and implementation costs, it shall take appropriate technical and organisational measures to prevent the unauthorised or unlawful Processing of

Personal Data and the accidental loss or destruction of, or damage to, Personal Data, and ensure a level of security appropriate to:

(i) the harm that might result from such unauthorised or unlawful Processing or accidental loss, destruction or damage;

(ii) the nature of the Personal Data protected; and

(iii) comply with all applicable Data Protection Legislation and its information and security policies, including the security measures required in 5.1.

14.2 The Customer warrants and represents that Hypertune's expected use of the Personal Data for the Business Purposes and as specifically instructed by the Customer will comply with the Data Protection Legislation.

This DPA has been entered into on the date stated in the Terms and Conditions.

Signed by [Insert Name of Director] [Print name]

for and on behalf of Insert [Name of **Customer**] Director

Signed by [Insert Name of Director] [Signature]

Signed by [Insert Name of Director] [Print name]

for and on behalf of [Insert Name of **Hypertune**] Director

Signed by [Insert Name of Director] [Signature]

Annex A: Personal Data processing purposes and details

Type	Description
Business Purposes	As described in the Terms and Conditions
Subject matter of Processing	The processing of Personal Data resulting from the provision of services by Hypertune under the Terms and Conditions
Nature of Processing	The Personal Data will be processed in the course of the operation of the Services.
Data Subject Types	Authorised Users
Personal Data Categories	Names and email addresses of Authorised Users.
Duration of Processing	As long as it is necessary for the performance of the service pursuant to the Terms and Conditions

Approved Sub-processor(s) List

Name	Purpose	Location
GCP	Cloud storage and hosting for Hypertune	UK
Google analytics	Site analytics	US
Cloudflare	Storing analytics data for customer projects	US
Bunny.net	Caching data from Cloudflare	Slovenia
Sendgrid	Sending customer email notifications	US
FullStory	Site analytics	US
Intercom	Customer support chat	US
Stripe	Payments processing	US
Linear	Issue tracking	US

Annex B: Security measures

Hypertune's description of its technical and organisational data security measures (TOMs)

Type	Description
System access controls	Hypertune enforces strict access controls based on the principle of least privilege, granting users only the permissions needed for their roles. Access is managed through a structured process with approvals and periodic reviews by the Information Security Group (ISG). Multi-factor authentication is required for privileged access, and unused or outdated permissions are promptly revoked to maintain security.
Data access controls	Hypertune enforces strict data access controls based on the principles of least privilege and need-to-know, granting only the minimum necessary access for job functions. Access provisioning and revocation are tracked and logged, with periodic reviews to ensure appropriateness. Multi-factor authentication and secure password policies are required, and privileged access is tightly regulated with separate administrative accounts. Third-party access is granted only with an active sponsor and reviewed regularly.
Encryption	Hypertune applies data encryption mechanisms at multiple points to mitigate the risk of unauthorized access to data at rest and in transit. ● **Encryption in transit.** To protect data in transit, Hypertune requires all inbound and outbound data connections to be encrypted using the TLS protocol. ● **Encryption at rest.** To protect data at rest, Hypertune uses industry standard encryption (AES-256) to encrypt all production data stored in our databases.
Data backups	Hypertune creates daily backups to ensure the ability to restore the availability and access to data in a timely manner in the event of a technical incident.
Data segregation	Hypertune implements segregation of environments (staging/production) and logic segmentation processes to manage data segregation.

Annex C: Standard Contractual Clauses (for transfers of Personal Data to third countries)

NOTE: Hypertune are based in the UK. Any transfer of Personal Data into the UK will not require Standard Contractual Clauses. On 28 June 2021 the EU Commission adopted decisions on the UK's adequacy under the EU's General Data Protection Regulation (EU GDPR) and Law Enforcement Directive (LED). In both cases, the European Commission has found the UK to be "adequate" ("Adequacy Decision").

Insert:

(1) EU Standard Contractual Clauses for the transfer of Personal Data where applicable.

(2) ICO UK Addendum where applicable.

(3) UK IDTA where applicable.

Annex D: Data Protection Officer contact details

Name: Michal Bock

Email: dpo@hypertune.com

Annex E: EU and Switzerland Data Protection Representative contact details

Hypertune has appointed DataRep as its Data Protection Representative for the purposes of EU GDPR in the EU/EEA and Federal Act on Data Protection (AS 2022 491) in Switzerland. If you want to raise a question to Hypertune, or otherwise exercise your rights in respect of your personal data, you may do so by:

- sending an email to DataRep at datarequest@datarep.com quoting <Hypertune Ltd> in the subject line,
- contacting DataRep on their online webform at www.datarep.com/data-request, or
- mailing your inquiry to DataRep at the most convenient of the addresses listed below. When mailing inquiries, it is essential that you mark your letters for 'DataRep' and not 'Hypertune', or your inquiry may not reach DataRep. Please refer clearly to Hypertune Ltd in your correspondence.

Country	Address
Austria	DataRep, City Tower, Brückenkopfgasse 1/6. Stock, Graz, 8020, Austria
Belgium	DataRep, Rue des Colonies 11, Brussels, 1000
Bulgaria	DataRep, 132 Mimi Balkanska Str., Sofia, 1540, Bulgaria
Croatia	DataRep, Ground & 9th Floor, Hoto Tower, Savska cesta 32, Zagreb, 10000, Croatia
Cyprus	DataRep, Victory House, 205 Archbishop Makarios Avenue, Limassol, 3030, Cyprus
Czech Republic	DataRep, Platan Office, 28. Října 205/45, Floor 3&4, Ostrava, 70200, Czech Republic
Denmark	DataRep, Lautruphøj 1-3, Ballerup, 2750, Denmark
Estonia	DataRep, 2nd Floor, Tornimae 5, Tallinn, 10145, Estonia
Finland	DataRep, Luna House, 5.krs, Mannerheimintie 12 B, Helsinki, 00100, Finland
France	DataRep, 72 rue de Lessard, Rouen, 76100, France
Germany	DataRep, 3rd and 4th floor, Altmarkt 10 B/D, Dresden, 01067, Germany
Greece	DataRep, Ippodamias Sq. 8, 4th floor, Piraeus, Attica, Greece
Hungary	DataRep, President Centre, Kálmán Imre utca 1, Budapest, 1054, Hungary
Iceland	DataRep, Kalkofnsvegur 2, 3rd Floor, 101 Reykjavík, Iceland
Ireland	DataRep, The Cube, Monahan Road, Cork, T12 H1XY, Republic of Ireland
Italy	DataRep, Viale Giorgio Ribotta 11, Piano 1, Rome, Lazio, 00144, Italy
Latvia	DataRep, 4th & 5th floors, 14 Terbatas Street, Riga, LV-1011, Latvia
Liechtenstein	DataRep, City Tower, Brückenkopfgasse 1/6. Stock, Graz, 8020, Austria
Lithuania	DataRep, 44A Gedimino Avenue, 01110 Vilnius, Lithuania
Luxembourg	DataRep, BPM 335368, Banzelt 4 A, 6921, Roodt-sur-Syre, Luxembourg
Malta	DataRep, Tower Business Centre, 2nd floor, Tower Street, Swatar, BKR4013, Malta
Netherlands	DataRep, Cuserstraat 93, Floor 2 and 3, Amsterdam, 1081 CN, Netherlands
Norway	DataRep, C.J. Hambros Plass 2c, Oslo, 0164, Norway
Poland	DataRep, Budynek Fronton ul Kamienna 21, Krakow, 31-403, Poland
Portugal	DataRep, Torre de Monsanto, Rua Afonso Praça 30, 7th floor, Algès, Lisbon, 1495-061, Portugal
Romania	DataRep, 15 Piaţa Charles de Gaulle, nr. 1-T, Bucureşti, Sectorul 1, 011857, Romania
Slovakia	DataRep, Apollo Business Centre II, Block E / 9th floor, 4D Prievozska, Bratislava, 821 09, Slovakia
Slovenia	DataRep, Trg. Republike 3, Floor 3, Ljubljana, 1000, Slovenia
Spain	DataRep, Calle de Manzanares 4, Madrid, 28005, Spain
Sweden	DataRep, S:t Johannesgatan 2, 4th floor, Malmo, SE - 211 46, Sweden
Switzerland	DataRep, Leutschenbachstrasse 95, ZURICH, 8050, Switzerland