Xponential7

PERSONAL DATA PROCESSING AGREEMENT

This Personal Data Processing Agreement (**DPA**), is entered into by and between Xponential7 Ltd and/or any Affiliate thereof ("**Xponential7**") and the customer who executes an agreement into which this DPA incorporated by reference, and/or any Affiliate thereof (the "**Customer**"). In this DPA, the Customer and Xponential7 are each a "**Party**" and collectively, the "**Parties**". The Parties have entered into an applicable Master Services Agreement, Insertion Order or Statement of Work (**Master Agreement**) that may require either or both Parties to process Personal Data. This DPA sets out the terms, requirements, and conditions on which the Parties will obtain, handle, process, disclose, transfer, or store Personal Data in connection with the Services under the Master Agreement.

In the course of providing the Services to Customer pursuant to the Master Agreement, Xponential7 may provide Customer with certain Personal Data (and may also process Personal Data on behalf of Customer). By executing the Master Agreement, the Customer enters into this DPA on behalf of itself and as agent on behalf of its Affiliates, if and to the extent (a) Xponential7 processes any Personal Data on behalf of Customer or (b) Customer receives any Personal Data from Xponential7, pursuant to the Master Agreement.

Xponential7 is the legal entity responsible for all data management obligations under this DPA, including compliance with applicable Privacy Laws. However, the operational processing of data, including any activities related to the delivery of Services, may be conducted under the brand names **'Demand7'** or **'GTM7'** or **'Automation7'** or **'Podcast7'**. All references to Xponential7 in this Agreement encompass data management and processing activities performed under the Demand7 or GTM7 or Automation7 or Podcast7 brand names. Legal accountability for data protection and compliance obligations remains solely with Xponential7.

In consideration of the mutual covenants and agreements hereinafter set forth and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties hereto agree as follows:

1. Definitions.

Terms such as **"(sub)process/(sub)processing**", "**data subject**", "**processor"**, "**controller**", "**personal data breach**", "**data protection impact assessment**", "**business**", "**service provider**", "**third party**" shall have the same meaning ascribed to them in Privacy Laws;

"**Affiliate**" means an entity which is controlling, controlled by or under common control or ownership with Xponential7 Solutions Limited or Customer (as applicable), where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.

"**Business Purpose**" means the services described in the Master Agreement or any other purpose specifically identified in the Annexes to this DPA.

"**Customer Data**" means any Personal Data that is provided or otherwise made available to Xponential7 by Customer and processed by Xponential7 in connection with the Services set forth in the Agreement.

"**Personal Data**" means any information or data provided or otherwise made available by Xponential7 to Customer or by Customer to Xponential7 that: (i) identifies, describes, locates or relates to an individual who can be identified directly or indirectly from that data alone or in combination with other information, (ii) the relevant Privacy Laws otherwise define as protected personal data or personal information. Personal Data includes both Customer Data and Xponential7 Data.

"**Privacy Laws**" means all applicable laws and regulations relating to the processing, protection, or privacy of the Personal Data, including where applicable, the guidance and codes of practice issued by regulatory bodies in any relevant jurisdiction. This includes, but is not limited to, all state and local privacy or information security Laws (including the California Privacy Rights Act (CPRA) amending the California Consumer Privacy Act of 2018 (Cal. Civ. Code §§ 1798.100 et seq.) ("**CCPA/CPRA**")) and the European Commission's General Data Protection Regulation (EU) 2016/679 as amended ("**GDPR**"); the EU Artificial Intelligence Act (Regulation (EU) 2024/1689, "**EU AI Act**") to the extent it applies to the processing of personal data in connection with AI

systems; and all legislation and Laws implementing or supplementing the GDPR in any country to which the same shall apply (collectively, "**EU Data Protection Laws**"), including the GDPR as retained in United Kingdom law by the European Union (Withdrawal) Act 2018 and amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 ("**UK GDPR**"); the EU ePrivacy Directive (Directive 2002/58/EC); and any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of the foregoing laws; in each case as may be amended or superseded from time to time.

"Restricted Transfer" means: (i) where the GDPR applies, a transfer of personal data from the European Economic Area ("**EEA**") to a country outside of the EEA which is not subject to an adequacy determination by the European Commission; and (ii) where UK GDPR applies, a transfer of personal data from the United Kingdom to any other country which is not subject based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018.

"Services" means services, products and/or other activities to be supplied to Customer or carried out by Xponential7 for Customer pursuant to the Master Agreement.

"**Standard Contractual Clauses (SCCs)**" means: (i) the European Commission's standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 for the transfer of personal data from the European Union to third countries pursuant to the GDPR. In the event that any provision of this DPA contradicts the SCCs, the SCCs shall prevail.

"**Xponential7 Data**" means any Personal Data that is provided or otherwise made available to Customer by Xponential7 in relation to the Services set forth in the Master Agreement.

This DPA is subject to the terms of the Master Agreement and is incorporated into the Master Agreement. Interpretations and defined terms set forth in the Master Agreement apply to the interpretation of this DPA. The Annexes form part of this DPA and will have effect as if set out in full in the body of this DPA. Any reference to this DPA includes the Annexes.

In the case of conflict or ambiguity between:

(a) any provision contained in the body of this DPA and any provision contained in the Annexes, the provision in the body of this DPA will prevail;

(b) the terms of any accompanying invoice or other documents annexed to this DPA and any provision contained in the Annexes, the provision contained in the Annexes will prevail;

(c) any of the provisions of this DPA and the provisions of the Master Agreement, the provisions of this DPA will prevail; and

(d) any of the provisions of this agreement and any executed Standard Contractual Clauses, the provisions of the executed Standard Contractual Clauses will prevail.

2. Personal Data Processing Roles and Purpose.

Roles of the Parties. For the purpose of this DPA: (i) with respect to Xponential7 Data, Xponential7 is a "controller" (under EU Data Protection Laws and reasonably equivalent term under Privacy Laws) and a "business" (under the CCPA/CPRA) and Customer is an independent and separate "controller" (under EU Data Protection Laws and reasonably equivalent term under Privacy Laws) and a "third party" (under the CCPA/CPRA); and (ii) with respect to Customer Data, Customer is the "controller" (under EU Data Protection Laws and reasonably equivalent term under Privacy Laws) and Xponential7 is the "processor" (under the CCPA/CPRA). Nothing in this DPA or the Master Agreement is intended to or shall create a relationship of joint controller between Xponential7 and Customer.

2.1 Xponential7 Data.

(a) Processing of Xponential7 Data. Customer shall only process Xponential7 Data for the Business Purposes. The Business Purposes shall include any restrictions communicated by Xponential7 to Customer with respect to the use of Xponential7 Data, including as required by Privacy Laws and/or in accordance with consents obtained from data subjects. Customer shall maintain the confidentiality of Xponential7 Data. Customer shall not process Xponential7 Data outside the scope of the Business Purposes. Processing of any Xponential7 Data outside the Business Purposes will require prior written

agreement between Xponential7 and Customer by way of written amendment to this DPA and may, where applicable, require additional consents to be obtained from data subjects.

(b) Customer acknowledges and agrees that it shall be an independent and separate controller, as applicable under Privacy Laws, of any Xponential7 Data and shall be solely responsible and solely liable for its processing of Xponential7 Data and for its compliance with all applicable laws, rules and regulations in connection with its use of Xponential7 Data, including, but not limited to, Privacy Laws.

(c) Duration of Processing. Subject to Privacy Laws and any restrictions communicated to Customer by Xponential7, Customer may process Xponential7 Data until it is no longer relevant for the purposes for which it was collected.

(d) Nature and Purpose of Processing. Customer, acting as a controller, may process Xponential7 Data in accordance with the applicable Business Purposes, which may include, without limitation, use of Xponential7 Data for the purposes of marketing to data subjects whose Personal Data is embodied in Xponential7 Data subject to any preferences communicated by such data subjects directly to Customer or to Xponential7 and reflected in restrictions communicated to Customer by Xponential7.

(e) CCPA/CPRA Requirements. To the extent CCPA/CPRA applies to the processing of Xponential7 Data, Customer hereby: (i) grants Xponential7 a right to conduct reviews, assessments, or take other reasonable and appropriate steps to ensure that the contracting party's use of personal information obtained under the contract is consistent with the business's CCPA/CPRA obligations, (ii) permits Xponential7 to take action to stop and remediate any unauthorized use of Xponential7 Data; and (iii) shall notify Xponential7 if it cannot meet its CCPA/CPRA obligations.

(f) The types of Xponential7 Data and Categories of Data Subjects are those set forth in Exhibit 1 of Annex A to this DPA.

2.2 Customer Data.

(a) Processing of Customer Data. Xponential7 shall maintain the confidentiality of Customer Data and shall only collect, use, retain, process or disclose Customer Data for the Business Purposes or otherwise in accordance with Customer's instructions. Xponential7 shall only process Customer Data in accordance with Customer's documented instructions and the terms of the Master Agreement (including this DPA). Processing of any Customer Data outside the Business Purposes will require the prior written agreement between Xponential7 and Customer by way of written amendment to this DPA. Xponential7 may promptly notify the Customer if, in its opinion, the Customer's instruction would not comply with the Privacy Laws.

(b) Duration of Processing. Xponential7 may process Customer Data for the duration specified in the Master Agreement, unless otherwise agreed upon in writing by the parties.

(c) Nature and Purpose of Processing. Xponential7 may process Customer Data in accordance with the applicable Business Purposes.

(d) Use of Artificial Intelligence. The parties acknowledge that the Services may involve the use of artificial intelligence tools for purposes including, but not limited to, data enrichment, content generation, and campaign optimisation. Where AI tools process Personal Data on behalf of the Client, such processing shall be subject to the same obligations and safeguards set out in this Agreement, including the requirement for appropriate human oversight.

(e) If a law requires Xponential7 to process or disclose Personal Data, Xponential7 must first inform the Customer of the legal requirement and give the Customer an opportunity to object or challenge the requirement, unless the law prohibits such notice.

(f) CCPA/CPRA Requirements. To the extent that the CCPA/CPRA applies to the processing of any Customer Data, Xponential7 shall not (i) sell the Customer Data, (ii) retain, use, or disclose the Customer Data for any purpose other than for the specific purpose of performing the services specified in the Master Agreement, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the

Agreement, or (iii) retain, use, or disclose the Customer Data outside of the direct business relationship between Xponential7 and Customer. Xponential7 will reasonably cooperate and reasonably assist Customer with meeting Customer's CCPA/CPRA compliance obligations and responding to CCPA/CPRA-related inquiries, including reasonably assisting the Customer in responding to verifiable consumer requests, taking into account the nature of Xponential7's processing, cost to Xponential7, and the information available to Xponential7. Xponential7 will limit the collection and use of Customer Data disclosed except as necessary to perform the Business Purposes for which Xponential7 was retained. Business Purposes in this context might also include Company's "operational" needs, such as auditing, detecting security incidents, fulfilling orders and transactions, processing payments. Both Parties will comply with all applicable requirements of the CCPA/CPRA when collecting, using, retaining, or disclosing Customer Data. Xponential7 certifies that it understands the CCPA/CPRA's restrictions and prohibitions on selling Customer Data and retaining, using, or disclosing Customer Data outside of the parties' direct business relationship, and it will comply with them.

(g) The types of Customer Data and categories of data subjects are those set forth in Exhibit 1 of Annex B to this DPA.

2.3 Compliance with Applicable Laws.

Each Party shall comply with its respective obligations under Privacy Laws in respect of the processing of all Personal Data. Without prejudice to the generality of the foregoing, where Customer is acting as a Controller in respect of Xponential7 Data, the Customer remains responsible for its compliance obligations under the applicable Privacy Laws, including providing any required notices and obtaining any required consents, and for the processing instructions it gives to Xponential7.

3. Assistance.

The Parties will reasonably assist each other with meeting their compliance obligations under Privacy Laws, while also considering the nature of each Party's processing and the information available to each Party.

4. Employees and Staff.

Each Party will limit Personal Data access to:

(a) those employees who require Personal Data access to meet each Party's respective obligations under this

Agreement; and

(b) the part or parts of the Personal Data that those employees strictly require for the performance of their duties.

Each Party will ensure that all employees who have access to or are involved in processing Personal Data:

(c) are informed of the Personal Data's confidential nature and use restrictions and are obliged to keep the Personal Data confidential;

(d) have undertaken training on the Privacy Laws relating to handling Personal Data and how it applies to their particular

duties; and

(e) are aware their duties and their personal duties and obligations under the Privacy Laws and this Agreement.

Each Party will take reasonable steps to ensure the reliability, integrity, and trustworthiness of any employee with access to the Personal Data.

5. Security

Each Party shall implement appropriate technical and organizational measures designed to safeguard Personal Data against unauthorized or unlawful processing, access, copying, modification, storage, reproduction, display, or distribution, and against accidental loss, unavailability, destruction, or damage. Each Party must take reasonable precautions to preserve the integrity of any

Personal Data it processes and to prevent any corruption or loss of the Personal Data, including but not limited to establishing effective back-up and data restoration procedures.

5.1 Xponential7's technical and organizational include, but are not limited to, the security measures set out in Exhibit 2 of Annex B.

6. Personal Data Breach.

Upon becoming aware of a confirmed Personal Data Breach, the Party experiencing the Personal Data Breach ("**Breached Party**") will without undue delay and in any event within seventy-two (72) hours, notify the other Party ("**Non-Breached Party**") of the Personal Data Breach.

6.1 Immediately following any unauthorized or unlawful Personal Data processing or Personal Data Breach, the Parties will co-ordinate and cooperate with each other to investigate, mitigate and remediate the Personal Data Breach. The Breached Party will provide such timely cooperation notification, and information as the Non-Breached Party may require in order for the Non-Breached Party to fulfil its reporting obligations under Privacy Laws.

The Parties agree that the Non-Breached Party has the sole right to determine:

(a) whether to provide notice of the Personal Data Breach to any Data Subjects, regulators, law enforcement agencies, or others, as required by law or regulation or in the Customer's discretion, including the contents and delivery method of the notice; and

(b) whether to offer any type of remedy to affected Data Subjects, including the nature and extent of such remedy.

7. Cross-Border Transfers of Personal Data.

If any Personal Data transfer between Xponential7 and the Customer requires execution of SCCs in order to comply with the Privacy Laws, the Parties will complete all relevant details in, and execute, the SCCs, and take all other actions required to legitimize the transfer, including implementing any needed supplementary measures or supervisory authority consultations.

The Parties agree that when the transfer of Personal Data is a Restricted Transfer it shall be subject to the appropriate SCCs as follows:

(a) If Xponential7 Data is subject to the Restricted Transfer, Xponential7 shall be the Data Exporter (as defined in the SCCs), Customer shall be the Data Importer (as defined in the SCCs), and Module 1 of the SCCs shall apply.

(b) If Customer Data is subject to the Restricted Transfer Customer shall be the Data Exporter (as defined in the SCCs), Xponential7 shall be the Data Importer (as defined in the SCCs), and Module 2 of the SCCs shall apply.

(c) In relation to the GDPR, the SCCs will be completed as follows:

(i) in Clause 7, the optional docking clause will apply;

(ii) in relation to 7.2(b) only: Clause 9, Option 2 will apply, and the time period for prior notice of subprocessor changes shall be thirty (30) days in accordance with Section 8 of this DPA.

(iii) In Clause 11, the optional language will not apply

(iv) In Clause 17, Option 1 will apply and the SCCs will be governed by the Republic of Ireland;

(v) In Clause 18(b), disputes shall be resolved in the courts of the Republic of Ireland;

(vi) Annex I of the SCCs shall be deemed completed with the information set out in Exhibit 1 of Annex A and/or B, as applicable to this DPA; and (vii) Annex II of the EU SCCs shall be deemed completed with the information set out in Exhibit 2 of Annex A and/or B, as applicable, to this DPA. (d) In relation to the UK GDPR:

(i) The Parties shall complete the UK Addendum to the SCCs, issued by the Information Commissioner's Office under s.119A(1) of the Data Protection Act 2018 ("**UK Addendum**"), and the SCCs as set forth above in section 7.2 shall apply to transfers of Personal Data. The UK Addendum shall be deemed executed between the transferring Customer and Xponential7, and the SCCs shall be deemed amended as specified by the UK Addendum in respect of the transfer of Personal Data.

The Parties will not make any Restricted Transfer unless the transfer complies with Privacy Laws and this DPA.

8. Subprocessors.

Customer hereby consents to the use of Xponential7 subprocessors listed in Exhibit 3 of Annex B to process Personal Data for the Business Purposes and as required to provide the Services. Xponential7 has entered into a written contract with each subprocessor that contains terms substantially the same as those set out in this DPA. Customer may opt-in to subprocessor email updates by sending an email to subprocessor@xponential7.com. Xponential7 shall update the subprocessor list at xponential7.com/legal/list-subprocessors with any changes to subprocessors and shall inform Customer at least thirty (30) days prior to any such change. Customer may object within thirty (30) days to any subprocessor change, provided such objection is based on reasonable grounds related to data protection. Where the subprocessor fails to fulfil its obligations under such written agreement, Xponential7 remains fully liable to the Customer for the subprocessor's performance of its agreement obligations.

The Parties consider Xponential7 to control any Personal Data controlled by or in the possession of its subprocessors.

9. Complaints and Data Subject Rights Requests.

Each Party must notify the other Party immediately 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 Privacy Laws.

Taking into account the nature of the processing, each Party must notify the other Party within 4 working days if it receives a request from a Data Subject for access to their Personal Data or similar request to exercise one of the Data Subject's personal data rights.

The Parties will co-operate and assist in responding to any complaint, notice, communication, or Data Subject request.

9.1 Xponential7 shall not disclose Customer Data to any Data Subject or to a third party other than at the Customer's request or instruction, as provided for in this DPA or as required by law.

10. Data Protection Impact Assessment.

Xponential7 shall provide Customer with reasonable assistance in order to conduct a data protection impact assessment for Customer Data in accordance with Privacy Laws.

11. Term and Termination

11.1 This DPA will remain in full force and effect so long as the Master Agreement remains in effect; or as otherwise required by Privacy Laws.

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

12. Data Return and Destruction

On termination of the Master Agreement or expiry of its term, Xponential7 will securely destroy or, if directed in writing by the Customer, return and not retain, the Customer Data related to this agreement in its possession or control.

If any law, regulation, or government, or regulatory body requires Xponential7 to retain any Customer Data Xponential7 would otherwise be required to return or destroy, it will notify the Customer in writing of that retention requirement, giving details of the documents or materials that it must retain, the legal basis for retention, and establishing a specific timeline for destruction once the retention requirement ends.

13. Records

13.1 Xponential7 will keep accurate records regarding any processing of Customer Data it carries out for the Customer sufficient to enable the Customer to verify Xponential7's compliance with its obligations under this DPA.

14. Audit

14.1 At least once per year, Xponential7 will audit its Customer Data processing practices and the information technology and information security controls for all facilities and systems used to demonstrate compliance with its obligations under this DPA and Privacy Laws.

14.2 Upon the Customer's written request, Xponential7 will make all of the relevant audit reports available to the Customer for review. The Customer will treat such audit reports as Xponential7's confidential information under this Agreement.

15. Warranties

Each Party warrants and represents that:

(a) its employees, subprocessors, agents and any other person or persons accessing Personal Data on its behalf are reliable and trustworthy and have received the required training on the Privacy Laws relating to the Personal Data; and

(b) it and anyone operating on its behalf will process the Personal Data in compliance with all applicable Privacy Laws and other laws, enactments, regulations, orders, standards, and other similar instruments; and

(c) it has no reason to believe that any Privacy Laws prevent it from providing any of the Master Agreement's contracted services; and

(d) considering the current technology environment and implementation costs, it will take appropriate technical and organizational measures to prevent the unauthorized 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 unauthorized or unlawful processing or accidental loss,

destruction, or damage; and

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

(iii) comply with all applicable Privacy Laws and its information and security policies, including the security

measures required in Section 5.

The Customer warrants and represents that Xponential7's expected use of Customer Data for the Business Purpose and as specifically instructed by the Customer will comply with all Privacy Laws.

ANNEX A

Exhibit 1 - Personal Data Processing Description

A. List of Parties

Controller(s) / Data Exporter(s):

1.	Name:	Xponential7 Ltd
	Address:	43 Tournay Road London SW6 7UQ United Kingdom
	Contact person's name, position and contact details:	Christian Iachini CEO & Founder Xponential7 Ltd / Managing Director Demand7 christian@demand7.ai
	Activities relevant to the data transferred under this DPA:	Performance of the Services by the Data Exporter to the Data Importer as specified in the Master Agreement.
	Role (controller/processor)	Controller
	Signature and date:	The Parties agree that the execution of the Agreement and/or the DPA shall constitute execution of the SCCs by both parties.

Processor(s) / Data Importer(s):

1.	Name:	Customer
	Address:	Customer's address as stated in the Master Agreement.
	Contact person's name, position and contact details:	Customer's account owner email address or the email address(es) for which Customer elects to receive legal communications.
	Activities relevant to the data transferred under this DPA:	Performance of the Services by the Data Exporter to the Data Importer as specified in the Master Agreement.
	Role (controller/processor)	Controller
	Signature and date:	The Parties agree that the execution of the Agreement and/or the DPA shall constitute execution of the SCCs by both parties.

B. Description of Transfer of Xponential7 Data:

Categories of data subjects whose Personal Data is transferred may include:	Customers of Xponential7 and/or end users of Xponential7 products and services; Prospective customers or sales prospects of Xponential7; Business partners and vendors of Xponential7; Employees, consultants or other contacts of Xponential7' customers, business partners and/or vendors; Employees, agents, advisors, contractors, freelancers of Xponential7; and/or; Any user authorized by Customer to use the Services.
Categories of Personal Data transferred may include:	First and last name; Business contact information (company, email, phone, physical business address); Personal contact information (email, telephone and/or mobile number); Employer; Title; Position; and/or Professional life data.
Sensitive data transferred (if applicable) and safeguards:	Not applicable.
The frequency of the transfer:	Continuous for the duration of the Services.
Nature of the processing:	As required to perform the Services, which may include, but is not limited to, organization, structuring, storage, adaptation or alteration, retrieval, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, and destruction.
Business Purposes of the data transfer and further processing:	To provide the Services as stated in an applicable Master Agreement and as otherwise to process Personal Data for the purpose of enabling Customer to provide its services to end-users and other personnel directed by the Customer.
The period for which the Personal Data will be retained:	As detailed in the Master Agreement.
For transfers to (sub-)processors, also specify subject matter, nature, and duration of the processing:	As permitted by the Master Agreement. In particular, transfers to hosting subprocessors may be required for storage and remote data processing, and these transfers shall align with the nature and duration specified in the Master Agreement.

ANNEX A

Exhibit 2 - Customer Technical and Organizational Security Measures

Organizational Security

1. Information Security Management Program

    a. Customer has an established, approved by management, and documented Information Security Management
    b. Program (evidence required) that is actively maintained, continually improved, and reviewed at least annually.

2. Customer has the following policies established, approved by management, and documented. The policies shall be continually improved, reviewed at least annually, and will require all Processor employees, contractors and interns to review and acknowledge annually. Evidence of these policies is required.

    a. Information Security Policy
    b. Acceptable Use Policy

3. Customer has the following policies established, approved by management, and documented. The policies shall be continually improved and reviewed at least annually. Evidence of policies is required.

    a. Access Control Policy
    b. Change Management Policy
    c. Mobile Device Management Policy
    d. Remote / Teleworker Policy

4. Risk Management

    a. Customer shall perform periodic risk assessments to evaluate the risk profile regarding the collection, storage, and use of Controller data.
        i. Risk Mitigation. Customer continually identifies and mitigates internal and external risks that could result in the compromise of confidential information or data;
        ii. Risk Assessment. Customer regularly conducts information privacy and security risk assessments in each area of proper operation;
        iii. Media Sanitization. Customer ensures that media sanitization conforms to NIST SP 800-88, Media Sanitization, or any successor standard.

5. Security Awareness and Training Program

    a. Customer has in place a Security Awareness Program that all employees are required to complete at hire and at least annually thereafter and is designed to enable employees and contractors to identify information privacy risks.

6. Business Continuity / Disaster Recovery

    a. Customer has in place a documented Business Continuity Plan and Disaster Recovery Plan.
    b. The plan must be tested, reviewed, and updated at least annually.
    c. The plan must be approved by management at least annually.

7. Physical Security

    a. Customer shall limit access to areas where Controller data is processed and maintain audit logs of any data access.
    b. Customer shall implement physical security protocols that will protect against the risks of physical penetration by malicious or unauthorized people, damage from environmental contaminants, and electronic penetration through active or passive electronic emissions.

8. Asset Management

    a. Customer has in place a system to manage and track all Processor owned or managed assets
    b. All assets used to manage or store the data must be protected against unauthorized access, disclosure, modification, destruction or interference.

Customers must provide appropriate security and protection from unauthorized access, damages and interference of assets based on classification, information sensitivity, and other factors.

Technical Security

1. Operating System / Software / Applications

    a. Customer shall have in place a method to communicate and/or push security patch updates for operating systems, software, and applications deployed in its environments.
    b. Critical patches and or updates shall be deployed within 30 days of release.

2. Access Credentials

    a. Customer shall secure its computer network using multiple layers of access controls to protect against unauthorized access. In particular, Customer shall have:

        i. Grouped network servers, applications, data and users into security domains;
        ii. Established appropriate access requirements within and between each security domain;
        iii. Implemented appropriate technological controls to meet those access requirements consistently; including (for example) firewalls.

    b. All employees who have access to or maintain Controller data:

        i. Shall have a unique user id/account
        ii. Shall not share user id/account with other users
        iii. Are required to authenticate with a second factor
        iv. Have roles and responsibilities defined and documented to incorporate the data protection control requirements including background checks to the extent permitted by applicable law.

    c. User accounts are required to:

        i. Have passwords expire at least every 180 days
        ii. Set to remember and not allow the use of at least the last 5 passwords
        iii. Where passwords are used, Processor requires the use of complex (upper/ lowercase alpha, special character, and a number) passwords
        iv. Lock a user account after 5 or less unsuccessful attempts
        v. Remain locked out for at least 15 minutes

d. Customer revokes any access of Customer's employee, contractor or third-party user to Controller data and facilities which process Controller data or provide access to Controller systems upon termination of their employment, contract or agreement, or adjust access upon a change of responsibility.

e. Customer shall appropriately leverage firewall infrastructure to segregate sensitive environments and restrict the use of insecure protocols. Network segments connected to the internet must be protected by a firewall which is configured to secure all devices behind it.

3. Customer shall have in place a method for managing and rotating access keys / SSH keys at a minimum of every 180 days.

4. Encryption

   a. Customer shall use full disk encryption on all corporate managed devices.
   b. Customer shall encrypt all Controller data in transit and at rest.

5. Backups

   a. If Customer performs backup of Controller data:
      i. Backups are required to be performed and stored in a secure location.
      ii. Backups shall be encrypted.

6. Intrusion Detection and Prevention

   a. Customer shall have in place an intrusion detection and prevention system in all corporate and production locations.

7. Anti-Virus / Anti-Malware

   a. Customer shall have in place anti-virus and anti-malware software on all Processor owned devices.
   b. The software shall be configured to:
      i. Update at least daily
      ii. Not allow local device level deactivation of the product
      iii. Perform full scans at least weekly
      iv. Report anomalies to security personnel who shall take appropriate action

ANNEX B

Exhibit 1- Personal Data Processing Description

A. List of Parties

Controller(s) / Data Exporter(s):

1.	Name:	Customer
	Address:	Customer's address as stated in the Master Agreement.
	Contact person's name, position and contact details:	Customer's account owner email address or the email address(es) for which Customer elects to receive legal communications.
	Activities relevant to the data transferred under this DPA:	Performance of the Services by the Data Importer to the Data Exporter as specified in the Master Agreement.
	Role (controller/processor)	Controller
	Signature and date:	The Parties agree that the execution of the Agreement and/or the DPA shall constitute execution of the SCCs by both parties.

Processor(s) / Data Importer(s):

1.	Name:	Xponential7 Ltd
	Address:	43 Tournay Road London SW6 7UQ United Kingdom
	Contact person's name, position and contact details:	Christian Iachini CEO & Founder Xponential7 Ltd / Managing Director Demand7 christian@demand7.ai
	Activities relevant to the data transferred under this DPA:	Performance of the Services by the Data Importer to the Data Exporter as specified in the Master Agreement.
	Role (controller/processor)	Processor
	Signature and date:	The Parties agree that the execution of the Agreement and/or the DPA shall constitute execution of the SCCs by both parties.

B. Description of Transfer of Customer Data:

Categories of data subjects whose Personal Data is transferred may include:	Customers of Customer and/or end users of Customer products and services; Prospective customers or sales prospects of Customer; Business partners and vendors of Customer; Employees, consultants or other contacts of Customer's customers, business partners and/or vendors; Employees, agents, advisors, contractors, freelancers of Customer; and/or; Any user authorized by Customer to use the Services.

Categories of Personal Data transferred may include:	First and last name; Business contact information (company, email, phone, physical business address); Personal contact information (email, telephone and/or mobile number); Employer; Title; Position; and/or Professional life data
Sensitive data transferred (if applicable) and safeguards:	Not applicable.
The frequency of the transfer:	Continuous for the duration of the Services.
Nature of the processing:	As required to perform the Services, and may include but is not limited to: organization, structuring, storage, adaptation or alteration, retrieval, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure and destruction.
Business Purposes of the data transfer and further processing:	To provide the Services as stated in an applicable Master Agreement and as otherwise to process Personal Data for the purpose of enabling Xponential7 to provide its services to end-users and other personnel directed by the Customer.
The period for which the Personal Data will be retained:	As detailed in the Master Agreement.
For transfers to (sub-)processors, also specify subject matter, nature, and duration of the processing:	As permitted by the Master Agreement. In particular, transfers to hosting subprocessors may be required for storage and remote data processing, and these transfers shall align with the nature and duration specified in the Master Agreement.

ANNEX B

Exhibit 2 – Xponential7 Technical and Organizational Security Measures

Area	Practices
Organization of Information Security	**Security Ownership**. Xponential7 has designated a person responsible for coordinating and monitoring Cybersecurity. **Security Roles and Responsibilities**. Xponential7 personnel with access to Customer Data are subject to confidentiality obligations. **Data Protection Office**: Xponential7 has appointed a Data Protection Officer.
Asset Management	**Asset Inventory**. Xponential7 maintains an inventory of all media on which Customer Data is stored. Access to the inventories of such media is restricted to Xponential7 personnel authorized in writing to have such access.
Huma Resources Security	**Security Training**. Xponential7 informs its personnel about relevant security procedures and their respective roles **Data Protection Training:** Xponential7 issues all staff with data protection training modules on induction and refresher training every year. Training modules cover data protection principles, data subject access request, data breach and keeping data secure.
Physical and Environment Security	**Physical Access to Facilities**. Xponential7 limits access to facilities where information systems that process Customer Data are located, to identified authorized individuals. **Protection from Disruptions**. Xponential7 uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference. **Component Disposal**. Xponential7 uses industry standard processes to delete Customer Data when it is no longer needed.

Communications and Operations Management	**Operational Policy**. Xponential7 maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Customer Data. **Data Recovery**: Xponential7 ensures off-site and on-site backup of customer data are maintained. **Malicious Software**. Xponential7 has anti-malware controls to help avoid malicious software gaining unauthorized access to Customer Data, including malicious software originating from public networks. **Data Beyond Boundaries.** Xponential7 encrypts, or enables Customer to encrypt, Customer Data that is transmitted over public networks. **Event Logging**. Xponential7 logs, or enables Customer to log, access and use of information systems containing Customer Data, registering the access ID, time, authorization granted or denied, and relevant activity.
Access Control	**Access Policy**. Xponential7 maintains a record of security privileges of individuals having access to Customer Data. **Access Authorization.** Xponential7 maintains and updates a record of personnel authorized to access Xponential7 systems that contain Customer Data. **Least Privilege.** Technical support personnel are only permitted to have access to Customer Data when needed. Xponential7 restricts access to Customer Data to only those individuals who require such access to perform their job function. **Authentication.** Xponential7 uses industry standard practices to identify and authenticate users who attempt to access information systems. Where authentication mechanisms are based on passwords, Xponential7 requires that the passwords are renewed regularly.
Information Security Incident Management	**Incident Response Process** Xponential7 has a management team and process for information security incidents as set forth in its detailed Information Security Incident Response Policy. Xponential7 provides notification of a security incident in compliance with appropriate laws, or regulations.
Data Protection	Xponential7 encrypts data during transmission and at rest. Xponential7 monitors data protection compliance and regularly tests the effectiveness of the measures in place. Xponential7 tests staff adherence to data protection and information governance policies and procedures.

Business Continuity Management	Xponential7 maintains emergency and contingency plans for the facilities in which Xponential7 information systems that process Customer Data are located. Xponential7 has a disaster recovery plan in place for the restoration of critical processes and operations of the Hosted Service at the hosting location from which the Hosted Service is provided.

Xponential7 Supplemental Measures

Area	Practices
Technical	The personal data is processed using strong encryption during transmission. Xponential7 has not purposefully created or changed its business processes in a manner that facilitates access to personal data or systems by third parties.
Contractual	Xponential7 monitors changes to local law and will inform the data exporter of any changes that will impact the maintenance of an 'essentially equivalent level of data protection' for the personal data transferred. Xponential7 has a process in place to assess local laws to ensure the legality of any disclosure of personal data.
Organizational	Xponential7 has a set of internal policies relating to requests from law enforcement agencies for access to personal data. Xponential7 provides a training program for all staff on procedures and processes for dealing with law enforcement agencies for requests to access personal data. Xponential7 keeps a register for requests from Public Authorities. Xponential7 conducts audits and allows inspections to verify if data was disclosed to public authorities. Xponential7 has contracted appointed a Data Protection Officer who is consulted on all high-risk transfers. Data Access and confidentiality policies and best practices in place and include regular review and audits.

ANNEX B

EXHIBIT 3 - XPONENTIAL7 SUBPROCESSORS

Xponential7 may use the following subprocessor(s) in the processing of Customer Data:
xponential7.com/legal/list-subprocessors