BENCHMARK GENSUITE®

DATA PROCESSING AGREEMENT

This Data Processing Agreement (this "**Agreement**") is between Benchmark Digital Partners, LLC, a Delaware limited liability company ("**Benchmark Digital**"), and [XXXX] (together with its subsidiaries and affiliates, the "**Customer**") in connection with that certain License and Service Agreement between Benchmark Digital and Customer dated [xxx] (the "**License and Service Agreement**").

This Agreement shall be effective as of the date of the License and Service Agreement and for the term specified under Article 4 hereunder.

1. DEFINITIONS AND QUALIFICATIONS. Except where explicitly stated otherwise in this Agreement, the terms "**Binding Corporate Rules**", "**Controller**", "**Data Breach**", "**Data Subjects**", "**Data Supervisory Authority**", "**Personal Data**", "**Processing**" and "**Processor**" shall have the same meaning in this Agreement as in both the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC" (hereinafter, the "EU-**GDPR**")

In addition, the following terms shall, within this Agreement, have the following meanings:

- "**Applicable Data Protection Laws**" means all and any laws, regulations and other domestic, European Union (EU) or international rules applicable to Processing of Personal Data in the context of the License and Service Agreement, including in particular the CCPA, the GDPR and all and any domestic data protection laws of EU Member States enacted to complement or specify the provisions of the GDPR, as well as all laws, regulations and other domestic, EU or international rules applicable to the processing of electronic communication data, the use of tracking technologies such as cookies and direct marketing (generally known as "**PECR**"), as applicable.

- "**CCPA**" means the California Consumer Privacy Act of 2018, as amended (Cal. Civ. Code §§ 1798.100 to 1798.199), the CCPA Regulations (Cal. Code Regs. tit. 11, §§ 999.300 to 999.337), and any related regulations or guidance provided by the California Attorney General. The term "Business Purpose" defined in the CCPA, carries the same meaning in this Agreement.

- "**Data Transfers**" means all and any transmission, copy, exchange or sharing of the Entrusted Personal Data to any person, entity or service located in a non-EU country which does not benefit from an adequacy recognition decision from the European Commission pursuant to Article 45 of the GDPR, and/or all and any access to the Entrusted Personal Data by any such person, entity or service.

- "**Entrusted Personal Data**" means all and any Personal Data received or accessed by Benchmark Digital in the context of the execution of this Agreement.

For all and any Processing carried out in the context of execution of the License and Service Agreement, the Parties hereby expressly recognize that the Customer is the Controller and Benchmark Digital is a Processor.

2. DESCRIPTION OF THE PROCESSING. For the sole purpose of the execution of the License and Service Agreement, the Customer hereby authorizes Benchmark Digital to carry out Processing of the Entrusted Personal Data as specified hereinafter (hereinafter the "**Entrusted Processing**"):

- **Purpose of the Entrusted Processing.** Benchmark Digital will collect, use, store and manage data, including personal data, related to among others Customer's employees, vendors, suppliers, and contractors for the term of the License and Service Agreement, and only for the Business Purposes set forth in the License and Service Agreement.

- **Nature of the Entrusted Processing.** The personal data to be processed includes personal data relating to among others Customer's employees as well as employees of prospective, current and former vendors, suppliers, and contractors of Customer for the purpose of meeting Customer's contractual and legal obligations. The processing activities are as described in the License and Service Agreement.

- **Categories of Entrusted Personal Data.** The personal data to be processed includes names, contact information (including home and work address, telephone numbers, email addresses, web addresses), citizenship, national and governmental identification information, work history, birth date, gender, language, special competencies, health data, certifications, job and business titles, familial relationships, training information, information of related persons, contractual information, business registrations, background investigations (collectively, the "**Entrusted Personal Data**").

- **Categories of Data Subjects.** The Data Subjects include individuals who are among others: agents, third parties, vendors, consultants or suppliers to Customer or Customer's employees as well as employees of agents, third parties, vendors, consultants or suppliers to Customer.

- **Duration of the Entrusted Processing.** The duration specified under Article 4 hereunder.

In addition, Benchmark Digital hereby informs the Customer of the following conditions for carrying out the Entrusted Processing:

- **Location of Benchmark Digital's servers.** Entrusted Personal Data may be stored by Benchmark Digital and/or its Processors authorized by the Customer in accordance with Article 3.1.7 hereunder in the following countries: Germany.

- **Benchmark Digital's Certification.** Benchmark Digital ISO-27001 certificate number is **ISMS-BE-113022** additionally, our subprocessors are certified as well with the ISO27001[1] standard as of the date of entering into the License and Service Agreement.

- **Benchmark Digital's Data Sharing Agreement.** Benchmark Digital hereby ensures that it has conducted group-internal Data Sharing Agreements.

- **Benchmark Digital's AI Solution.** Solution has been developed by Benchmark Digital and is hosted in its servers, Customer's data will be processed exclusively by Benchmark Digital no third-party or subprocessor will be involved for this specific purpose.

- **List of Benchmark Digital's Processors.** The list of Benchmark Digital's Processors authorized by the Customer in accordance with Article 3.1.7 hereunder as of the date of entering this Agreement is attached under Annex A of this Agreement.

- **Data Protection Officer.** Benchmark Digital has appointed a Data Protection Officer, who may be contacted at DPO@benchmarkdigital.com.

The specifications described under this Article 2 may only be modified upon the Customer's documented instructions or, as applicable, with the Customer's prior written authorization.

Benchmark Digital shall inform the Customer of any change in the conditions of performance of its activities or its Processors' activities which may modify or otherwise impact in any way the specifications of the Entrusted Processing as described under this Article 2, and shall obtain the Customer's prior written authorization for such a change before implementing it. Any such change, as

[1] https://www.cloudflare.com/trust-hub/compliance-resources/
https://d1.awsstatic.com/certifications/iso_27001_global_certification.pdf

well as any new Entrusted Processing, may only be implemented or carried out in compliance with this Agreement.

3. OBLIGATIONS. Each Party commits to perform the License and Service Agreement in compliance with the Applicable Data Protection Laws, and to comply with its own obligations pursuant to the Applicable Data Protection Laws at all time in the context of the execution of the License and Service Agreement.

3.1. SERVICE PROVIDER'S OBLIGATIONS

3.1.1 **Processing on Customer's Documented Instructions.** Benchmark Digital shall process the Entrusted Personal Data upon the Customer's documented instructions only, including with regard to Data Transfers, unless required to do so by EU law or domestic law of any EU Member State to which the processor is subject; in such a case, Benchmark Digital shall inform the Customer of that legal requirement before processing, unless that law prohibits such information on significant grounds of public interest.

The Parties hereby expressly recognize that this Agreement and the License and Service Agreement are the Customer's documented instructions for the purpose of the preceding paragraph.

3.1.2 **Service Provider's Assistance to Customer.** Benchmark Digital shall take all necessary and/or relevant measures to assist the Customer in complying with its obligations pursuant to the GDPR, and the CCPA, i.e. in particular the Customer's obligation to handle and answer Data Subjects' requests to exercise their rights, the Customer's obligations related to the security of the Entrusted Processing and to notifications of Data Breaches, the Customer's obligation to maintain records of processing activities as the Controller and/or as the Processor, and the Customer's obligations to conduct Privacy Impact Assessments ("**PIAs**") and to consult with Supervisory Authorities.

The aforementioned measures shall in particular include, without limitation, Benchmark Digital's maintaining of comprehensive documentation of the conditions in which it shall carry out the Entrusted Processing and of the incidents that occur in relation to the Entrusted Processing, Benchmark Digital's notification to the Customer of any relevant element of this documentation without undue delay upon the Customer's first request.

With regards to Data Subjects' requests to exercise of their rights, Benchmark Digital shall redirect any such request that it might receive to the Customer, without undue delay, and not answer any such request by itself, except where otherwise instructed by the Customer in writing. Benchmark Digital shall comply without undue delay to any of the Customer's documented instructions regarding the implementation of a Data Subject's request, e.g. instructions to correct or erase certain Entrusted Personal Data.

3.1.3 **Security of Entrusted Processing.** Benchmark Digital shall take and maintain all necessary and/or appropriate technical, logical and organizational measures so as to ensure an adequate level of security of the Entrusted Processing with regard to (i) the then current state of the art, (ii) the specifications of the Entrusted Processing as described under Article 2 here above and/or in the Customer's documented instructions (in particular if these specifications include the processing of sensitive data or of personal data subject to specific requirements under Applicable Data Protection Laws), and in any case (iii) all security requirements provided by or resulting from Applicable Data Protection Laws, the doctrine and case law of Supervisory Authorities, as well as any laws, regulations or other domestic, EU or international rules providing for obligations or requirements having a direct or indirect impact on the security of processing of Personal Data or to IT systems.

As of the date of entering into this Agreement, Benchmark Digital warrants that it has implemented the measures listed in Annex 2 hereunder. Benchmark Digital shall maintain those measures and update them as applicable and shall implement new measures, if necessary, for the whole duration of this Agreement so as to ensure an adequate level of security with regard to the

aforementioned criteria at all times, and shall under no circumstances reduce or deprecate this level of security.

3.1.4 **Confidentiality of Entrusted Personal Data.** Benchmark Digital shall take all measures to limit access to the Entrusted Personal Data to the sole persons among its employees and Processors who need to access it to perform their duties in the context of the execution of the License and Service Agreement (hereinafter the "**Authorized Recipients**").

Benchmark Digital warrants that the Authorized Recipients comply with the provisions of this Agreement and the provisions of Applicable Data Protection Laws. Benchmark Digital shall provide the Authorized Recipients with adequate awareness, sensitization and training programs relating to their obligations resulting from the aforementioned provisions, and/or ensure that such programs are provided to the Authorized Recipients.

Benchmark Digital shall ensure that all and any Authorized Recipients are bound by appropriate confidentiality obligations with regard to the Entrusted Personal Data, either through Non-Disclosure Agreements or through enforceable statutory, legal or regulatory confidentiality obligations imposed on the Authorized Recipients.

In the event that Benchmark Digital is ordered by any jurisdiction, authority, administration or other public agent (hereinafter an "**Authority**") to allow access to Entrusted Personal Data, or to disclose or transmit a copy of the Entrusted Personal Data, Benchmark Digital shall take all necessary and/or appropriate measures to secure the confidentiality of the Entrusted Personal Data, including at least the following measures:

- Benchmark Digital shall notify the Customer of the order received (if and to the extent such notification is not explicitly prohibited by the order itself or by applicable laws or regulations) and strictly comply with the Customer's documented instructions with regard to that order;

- Or, as applicable, Benchmark Digital shall use all reasonable means either to (i) redirect the Authority to the Customer for obtaining an answer to the order received, (ii) oppose the prohibition to notify the Customer of the order received, or (iii) oppose the validity or lawfulness or the order received;

- In any case, Service Provider shall abstain from disclosing the Entrusted Personal Data unless if presented with a definitive judicial decision or order.

In the event that the disclosure of the Entrusted Personal Data to an Authority would require a Data Transfer, Benchmark Digital shall immediately inform the Customer and shall enter into appropriate Standard Contractual Clauses as referred to in Article 3.1.8 hereunder, if no such Standard Contractual Clauses are already entered into.

3.1.5 **Customer's information and right of audit.** Benchmark Digital shall provide Customer, upon the Customer's request, with all and any document or evidence necessary and/or appropriate to prove Benchmark Digital's compliance with its obligations under this Agreement including, without limitation, its obligations relating to the security of the Entrusted Processing and confidentiality of the Entrusted Personal Data. The cost of the audit and any other costs incurred by Benchmark Digital will be borne by the Customer. These documents and evidence may in particular consist of certificates or affidavits from professional third parties, or of reports of audits carried out by Benchmark Digital itself, without prejudice to the Customer's right of audit as described hereunder. Benchmark Digital recognizes and agrees that these documents and evidence may be transferred or disclosed to any competent jurisdiction or authority in order to prove compliance of the Entrusted Processing with Applicable Data Protection Laws.

The Customer may at any time choose to conduct or have any third party (hereinafter a "**Third Party Auditor**") conduct an audit of Benchmark Digital in order to verify Benchmark Digital's compliance with its obligations under this Agreement including, without limitation, its obligations relating

to the security of the Entrusted Processing and confidentiality of the Entrusted Personal Data. Benchmark Digital recognizes and agrees that the audit operations may justify access to all and any information, including confidential information, necessary to conduct the aforementioned verification. Benchmark Digital shall allow and facilitate the conduct of these audit operations, including by providing personnel and all necessary and/or appropriate information for that purpose.

The audits referred to in the preceding paragraph may only be conducted during normal business hours, and are conditional upon the Customer's prior notification of its intention to conduct an audit to Benchmark Digital at least one (1) week before the conduct of the audit, comprising the designation of the persons or entities mandated by the Customer to conduct the audit. In the event that the audit is conducted by a Third Party Auditor, the Customer warrants that this Third Party Auditor offers sufficient guarantees in terms of confidentiality with regard to the information that it could access during the audit.

Benchmark Digital may object to the designation of a specific Third Party Auditor if, for compelling reasons relating to its particular situation (e.g. if the Third Party Auditor is a competitor of Benchmark Digital), the conduct of the audit by this Third Party Auditor is manifestly likely to cause Benchmark Digital harm. Under no circumstance shall the exercise of this right to object aim at or result in hindering the Customer's right to audit Benchmark Digital.

3.1.6 **Data Breaches.** Benchmark Digital shall notify the Customer in writing and without delay of any Data Breach impacting or otherwise concerning the Entrusted Personal Data, and in any case within seventy-two (72) hours counting from the first moment at which Benchmark Digital is aware of the Data Breach. Benchmark Digital shall also take and/or propose to Customer, without undue delay, any necessary and/or relevant measures in order to (i) identify the origin, the nature, the scope and the consequences of the Data Breach, (ii) remedy the Data Breach and (iii) limit or neutralize the consequences of the Data Breach.

The information notified to the Customer pursuant to the preceding paragraph must include at least the following elements:

- A description of the Data Breach including at least: the nature and origin of the Data Breach; the categories of the Entrusted Personal Data impacted or otherwise concerned by the Data Breach; an estimation of the number of Data Subjects affected;

- The name and contact details of the Data Protection Officer or of any other person whom the Customer may contact to obtain further information and follow-up regarding the investigation and remedy of the Data Breach;

- A description of the likely and possible consequences of the Data Breach;

- A description of the immediate measures taken and / or proposed long-term measures to be taken by Benchmark Digital in order to remedy the Data Breach and to limit or neutralize its consequences.

In the event that all the aforementioned elements are not immediately known or available, Benchmark Digital commits to at least notify the Customer of the occurrence of the Data Breach within the period specified here above, and to communicate the additional information without delay as soon as it is available.

Without prejudice to the above minimal obligations, Benchmark Digital shall use its best efforts to assist the Customer in complying with its obligations regarding the notification of the Data Breach to the Supervisory Authorities and to Data Subjects, as applicable.

3.1.7 **Subprocessing.** Benchmark Digital may only subcontract all or part of its obligations under the License and Service Agreement with the Customer's prior written authorization. This authorization shall be given on a case-by-case basis for each Processor, after Benchmark Digital has

notified the Customer of its intention to engage this Processor. The Customer's prior written authorization must also be obtained before replacing or dismissing any then current Processor. Customer's right to authorize or refuse Benchmark Digital's Processors shall not aim at hindering all and any possibility of subcontracting under this Article. In the event that no agreement is reached on the identity of a Processor to be engaged, and the execution of the License and Service Agreement cannot be achieved for that reason, the Customer shall have the right to terminate the License and Service Agreement without any charges or penalty other than the outstanding sums relating to Benchmark Digital's tasks that have been completed up to that time.

In any case, Benchmark Digital may only engage Processors allowing it to ensure compliance of the Entrusted Processing with Applicable Data Protection Laws. Processors who are subcontracted must in this respect (i) offer adequate guarantees with regard to applicable obligations in terms of the security of the Entrusted Processing and of confidentiality of the Entrusted Personal Data, and (ii) commit to same or at least equally strict obligations as the ones imposed on Benchmark Digital under this Data Processing Agreement. In particular, Processors may only engage their own Processors under the conditions set forth in this Paragraph.

3.1.8 **Cloud-Based SaaS Solution**. Benchmark Gensuite is provided as a Software as a Service (SaaS) solution. All software, infrastructure, and processing services for Benchmark Gensuite are entirely cloud-based and hosted by Benchmark Digital. Customer shall not be responsible for any on-premise hardware, software, or IT infrastructure to access or utilize Benchmark Gensuite. Benchmark Digital shall be solely responsible for the provisioning, maintenance, and operation of all cloud-based services, servers, storage, and networking required to deliver the Benchmark Gensuite solution to Customer.

3.1.9 **Data Transfers.** Benchmark Digital shall be held as Data Importer and will satisfy the four following cumulative conditions: (i) Benchmark Digital has informed the Customer of the location of the intended recipients; (ii) Benchmark Digital has informed the Customer of the purpose for the Data Transfer; (iii) Customer's prior written consent for the intended Data Transfer; and (iv) the appropriate guarantees are provided for the Data Transfer, Customer and Benchmark Digital have entered into Controller-to-Processor (Module 2) Standard Contractual Clauses adopted by the European Commission or adopted by a Supervisory Authority and approved by the European Commission pursuant to Article 46.2. c) and d) of the GDPR, as attached in Annex C.

In the event that in Benchmark Digital's reasonable opinion the Data Transfer may fall within the scope of one of the exemptions provided for under Article 49 of the GDPR, Benchmark Digital shall notify the Customer accordingly, it being understood that the Customer alone shall retain full authority to decide whether it is necessary to implement the aforementioned appropriate guarantees.

In the event that the instrument used to provide the aforementioned appropriate guarantees disappears, is deemed invalid or cannot be relied on for any other reason, Benchmark Digital commits to suspend immediately all affected or concerned Data Transfers, and shall offer the Customer acceptable alternative temporary solutions including storage of the Entrusted Personal Data within the European Union. Furthermore, in such circumstances, the Parties shall negotiate in good faith so as to agree upon a solution to restore quickly the appropriate guarantees for the Data Transfer. Except in the case of *force majeure*, this situation shall not justify the suspension of the execution of the License and Service Agreement or its termination by Benchmark Digital.

3.1.10 **Deletion/Return of Entrusted Personal Data.** Benchmark Digital shall, at the conclusion of the License and Service Agreement, irreversibly delete all the Entrusted Personal Data still in its possession or under its control, or return all such Entrusted Personal Data to the Customer in an unaltered and reusable form, and shall instruct all its Processors to do the same.

In the event that no documented instructions are provided by Customer for the purpose of the preceding paragraph, Benchmark Digital shall proceed with the deletion of the Entrusted Personal Data.

Deletion or return of the Entrusted Personal Data, for the purpose of the preceding two paragraphs, means the deletion or return, in particular, of all files, documents, medias or supports of any nature containing the Entrusted Personal Data under this Data Processing Agreement.

In the event of the deletion of the Entrusted Personal Data, Benchmark Digital shall retain all necessary and/or appropriate evidence of such deletion, in any relevant form, including in particular certificates or affidavits from professional third parties, and shall communicate all such evidence to Customer upon the latter's first request.

3.1.11 **Benchmark Digital's Warning to Customer.** In the event that, in Benchmark Digital's reasonable opinion, a Customer's documented instruction relating to Entrusted Processing may be deemed unlawful with regard to Applicable Data Protection Laws, or may cause infringement of Applicable Data Protection Laws, Benchmark Digital shall immediately notify the Customer, it being understood that the latter shall remain solely in charge of and responsible for deciding whether the instruction is to be followed eventually.

3.1.12 **Insurance.** Benchmark Digital warrants that, as of the date of entering into this Agreement, it has all sufficient insurance policies in order to cover all liabilities incurred under this Agreement, and that it shall maintain these policies, or at least equally comprehensive policies, for the whole term of this Agreement as defined under Article 4 hereunder.

3.2. CUSTOMER'S OBLIGATIONS

3.2.1 **Lawfulness of Entrusted Processing.** The Customer, as Controller, remains solely responsible for the lawfulness of the Entrusted Processing, especially with regard to the principles and obligations in relation to legal grounds for the Entrusted Processing and the information of Data Subjects under Applicable Data Protection Laws.

3.2.2 **Communication with Data Subjects and Supervisory Authorities.** Except where otherwise instructed by the Customer and with regards to requirements imposed by applicable laws and regulations, the Customer shall have sole and exclusive control over communication with the Data Subjects and the Supervisory Authorities regarding the Entrusted Processing.

3.2.3 **Benchmark Digital's AI advisors and solutions.** The Customer shall not, directly or indirectly, nor permit any User or third party to: (a) reverse engineer, decompile, refurbish, disassemble or otherwise attempt to discover the source code or underlying ideas or algorithms of the AI solutions; (b) modify, translate, or create derivative works based on the AI solutions; (c) rent, lease, distribute, sell, resell, assign, or otherwise transfer rights to use the AI solutions; (d) use the AI solutions for time-sharing or service bureau purposes or otherwise for the benefit of any third party; (e) remove any proprietary notices or labels on the AI solutions; (f) publish or disclose to third parties any benchmarking or performance studies involving the AI solutions without Benchmark Gensuite's prior written consent; (g) use the AI solutions for any purpose other than their intended purpose; (h) interfere with or disrupt the performance of the AI solutions or the data contained therein; (i) introduce any open source software into the AI solutions; or (j) attempt to gain unauthorized access to the AI solutions or related systems or networks.

4. TERM. This Agreement is entered into and will remain in force until complete the deletion or complete return of all the Entrusted Personal Data to the Customer in compliance with Article 3.1.9 above.

5. PRECEDENCE. In the event of a conflict between the provisions of this Agreement and the provisions of the License and Service Agreement, the Parties agree that the provisions of this Agreement shall prevail.

6. MODIFICATION. This Agreement may only be modified through written agreement signed by both Parties.

IN WITNESS WHEREOF, this Agreement is entered into and becomes a binding part of the Agreement with effect from the Agreement Effective Date first set out above.

SIGNING PARTS:

CUSTOMER	**Benchmark Digital Prtners LLC**
Customer's approved signature	Jason Krueger
Title	Chief Data Security & IT Officer
Date	*Date*
_____	_____

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter:

1. Name: click here to enter text

   Address:

   Contact person's name, position and contact details: click here to enter text

   Activities relevant to the data transferred under these Clauses: Data entry and provision into the Benchmark Digital Software System for the purposes of EHS management / ESG Management

   Role (controller/processor): Controller

Data importer:

1. **Name**: Benchmark Digital Partners LLC
   Address: 4680 Parkway Drive STE 400 Mason Ohio 45040

   Contact person's name, position and contact details: Jason Krueger, Infrastructure & IT Security Officer, DPO@benchmarkdigital.com

   Activities relevant to the data transferred under these Clauses: The data importer is Benchmark Digital (the Supplier). The data importer provides a SaaS based solution which can be accessed by the Data importer's employees, other workforce and representatives of Data Importer's contractors who have been granted access into the solution by Data importer

   The following entities are part of a unique processor under the same instructions, confidentiality standards and depend upon the same data protection officer

Benchmark list of Parties	Address
Benchmark Digital Partners LLC.	4680 Parkway Drive Suite 400 Mason OH 45040 **USA**
Benchmark Digital Partners Pty. Ltd.	Level 3 9-13 Castlereagh Street Sydney NSW 2000 **Australia**
Benchmark Digital Partners Canada ULC	5353 Dundas Street West Unit 302 Toronto, ON M9B 6H8 **Canada**
Shanghai Benchmark Digital Partners LTD	Suite 108, BoYun Road No. 2 PuDong District Shanghai, **China** 201203
Benchmark Digital México, S. de R.L. de C.V.	Blvd a Zacatecas #845, Interior #301 Trojes de Alonso, Centro Comercial Punto45, C.P 20116 Aguascalientes, AGS **Mexico**
Benchmark ESG Private Ltd.	No 22, 2nd Floor, Sankey Road, VK Commercial Complex (Future Group Building) Opp: BDA Head Office Bangalore, Karnataka – 60020ka **India**
Benchmark Digital Partners UK Ltd	Suite 304, Parkway House Sheen Lane East Sheen London SW148LS **United Kingdom**
Benchmark Digital Partners SARL	54 RUE DE BITCHE PARIS LA DEFENSE 7 92400 COURBEVOIE **France**
Benchmark Digital Partners s.r.o.	Zochova 6-8 811 03 Bratislava **Slovakia**
Benchmark Digital Partners GmbH	Thomas-Wimmer-Ring 17 80539 Munich **Germany**

B. DESCRIPTION OF TRANSFER

Appropriate security and control measures are in place, Benchmark is certified as ISO 27001 Compliant (**ISMS-BE-113022**).

Benchmark Party	**Location (country)**	**Services provided**
Benchmark Digital Partners LLC.	United States	Administration/Support Services (Tier 3 sales escalations)
Benchmark Digital Partners SARL	France	Sales & Leadership Engagement Services (Tier 3 sales escalations)
Benchmark Digital Partners GmbH	Germany	Sales & Leadership Engagement Services (Tier 2 sales & leadership escalations)
Benchmark Digital Partners S.R.O.	Slovakia	Sales & Leadership Engagement Services (no escalations)
Benchmark Digital Partners UK Ltd	U.K.	Sales, Service, Leadership Engagement Services (Tier 2 service and leadership escalations)
Benchmark Digital S DE RL DE CV	Mexico	Sales, Services, Data base Administration, Application Development, HR, Operations, Leadership Engagement (Tier 1 service, database, HR escalations) (Tier 2 sales, application dev, leadership escalations)
Benchmark Digital Partners Canada ULC	Canada	Sales, Services, Application Development, Operations, Leadership Engagement (Tier 1 sales and application development escalations) (Tier 3 operations and leadership escalations)
Benchmark ESG Private Ltd.	India	Sales, Services, Data base Administration, Application Development, HR, Operations, Leadership Engagement (Tier 1 service, database and application dev, leadership escalations) (Tier 2 sales, HR, operations escalations)
Shanghai Benchmark Digital Partners LTD	China	Sales, Services, Data base Administration, Application Development, HR, Operations, Leadership Engagement (Tier 2 escalations for all)
Benchmark Digital Partners Pty. Ltd.	Australia	Sales, Services, Application Development, Leadership Engagement (Tier 3 escalations for all)

Tier escalation doesn't involve Personal Data transfers by default, on a system error response team might have access to registries that can potentially contain such data, nevertheless information would

not be transferred or stored in a remote location, consults are on cloud-based environment and will serve problem solving purposes only. Any access related to the aforementioned cases would be logged.

International data transfers aren't a recurrent activity linked to any processing activity. Complete databases will not be transferred, data access will be on a single record basis as needed. Data transfers outside the USA will be extraordinary activities that will only take place in specific situations like:

- Ticket escalation regarding user issues.
- Ticket escalation related to system issues.
- Specific analysis.

Cases mentioned above do not require any printing or physical data transfer, Benchmark's internal data protection policies explicitly prohibit such practices.

Categories of data subjects whose personal data could be transferred:

- Employees
- Contractors
- Customers or consumers
- Suppliers

For most cases, data won't be stored in third countries, most of the times it will only be accessed remotely using proper controls, data in transit is encrypted through HTTPS and latest secure version of TLS. If absolutely necessary, the assets to where data will be imported for ticket attendance are:

- Software Systems
- Applications Server
- Data Bases
- Personal Computers

Benchmark relies on subsidiaries in different global locations which are under the same board of directors and follow the institutional guidance, offices are not independent in the decisions regarding additional data processors or using third parties. Offices established don't have general access granted to any customer's information, as previously stated access would take place in tiered escalation situations where it is completely necessary. There are specific binding contracts that regulate the relationship and establishes obligations. For data transfers all controls are in place to guarantee that information will not be disclosed.

Benchmark's escalation protocol is time and severity dependent; escalation and handoff will be handled accordingly. Benchmark understands that our customers necessities should be addressed without undue delay.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Measures of pseudonymisation and encryption of personal data

All PII data is encrypted at rest at the field level with a unique AES 256-bit key generated specifically for each customer, which is stored in a secret server, rotated out annually. All data in transit is encrypted through HTTPS with the latest secure version of TLS. Benchmark doesn't use pseudonymisation.

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

- Benchmark Digital ESG application availability (outside the scheduled maintenance outage window) is expected to be 99% or greater.
- In the event of a server or data loss, Benchmark Digital shall restore the information stored by Customer within its instance of the Benchmark Digital Application from the tape backups and transaction log backups, or make commercially reasonable efforts to recreate such data, within a reasonable period of time.
- Incident detection is reported on application, server and infrastructure levels. User facing incident reporting is done in the form of application error and bug reporting.
- Incident Response table top tests are performed monthly, logged in Benchmark Digital's compliance calendar tool.

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

- Backups are stored at a geographically separated location from production facility.
- Backups are performed daily. Restoration procedures are tested with the disaster recovery plan or as needed.
- Incident Response Strategy
    1. Upon discovery, Benchmark Digital personnel uses emergency contact list to escalate to incident response team.
    2. Incident Response Team analysis the incident and assess the impact and criticality of the incident.
    3. Take action as appropriate to stop or contain incident (e.g. disconnect system, block connection, etc.).
    4. Develop a response strategy based upon findings and coordinate communication with applicable parties.
    5. Restore affected system to their original state while maintaining all applicable evidence related to the incident.
    6. Conduct root cause analysis on incident and determine necessary preventive/corrective actions.
    7. Update applicable documentation and/or policies based on root cause analysis and preserve evidence.
    8. Assess impact to customers, damage and cost associated the incident.
    9. Notify proper external agencies, as appropriate to the type of incident.

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

Benchmark Digital monitors its system, the Service, Software, and its procedures for security breaches, violations and suspicious (questionable) activity. All commercially reasonable measures are in place to secure and defend the Service, Software, its location and equipment. Benchmark Digital periodically tests its systems for potential areas where security could be breached and will notify Subscribers immediately in writing upon learning of any security breach or suspicious activity that may compromise the security of any Subscriber Data or Confidential Information.

As needed, Benchmark Digital engages a third party vendor ("Testing Company") to perform penetration and vulnerability testing ("Penetration Tests") with respect to the Service and Software. The objective of such Penetration Tests is to identify design and/or functionality issues in applications or infrastructure of the Service or Software which could expose Subscriber's or users' assets or data to risks from malicious activities. Penetration Tests probe for weaknesses in applications, network perimeters or other infrastructure elements as well as weaknesses in process or technical countermeasures relating to the Service or Software that could be exploited by a malicious party.

Within a reasonable timeframe, Benchmark Digital notifies Subscriber in writing of any critical security issues that were revealed during such Penetration Test which have not been fully remediated. Once the issues have been mitigated, Benchmark Digital subsequently engages the Testing Company to perform an additional Penetration Test within a reasonable period thereafter to ensure continued resolution of identified security issues and results are made available to the Subscriber upon request.

Measures for user identification and authorisation

Single Sign On (SSO) or Active Directory login integration is the recommended approach for Intranet-accessed instances. The standard integration configuration involves authentication on a designated Company server within the customer Intranet. The user accessing a Benchmark URL is re-directed to the authentication server for authentication, the authenticated user ID is encrypted packet and then passed back to the Benchmark URL. The user's permissions are then validated within Benchmark for the application and business scope being accessed. User passwords are not stored in the Benchmark business database when authentication is via a Company SSO/Active Directory server. For Intranet-accessed instances, new users can automatically begin register within Benchmark Digital on identification and login authentication by the company login server.

For Internet-accessed instances, users login via a custom Benchmark Digital user name (set to their email address) and a user-designated password that is hashed with SHA1 and stored within the Benchmark business SQL database. Password resets and updates to the Benchmark user account password are managed by the user and are never emailed or made visible to any user. New users must submit a request with their email address. If the address is matched within the manually-administered Company Directory, a registration email is sent to the email account containing an authentication link to complete the registration process and set the password. If not matched, the request is forwarded to the designated administrator who can validate the request and then initiate the process by adding the record to the Benchmark user database and the Company Directory.

Measures for the protection of data during transmission

Access to databases would be under strict security measures (VPN) and Benchmark guarantees that employees who access it comply with data protection training and binding non disclosure contracts have been signed

Measures for the protection of data during storage

PII data is encrypted at rest at the field level with a unique AES 256-bit key generated specifically for each customer, which is stored in a secret server and, rotated out annually.

Measures for ensuring physical security of locations at which personal data are processed

All data hosting facilities are monitored by video surveillance on a 24 hour by 7 day, 365 days per year basis in accordance with the Benchmark Digital IT and Data Security Policy. Records are maintained providing evidence of these safeguards by Benchmark Digital's hosting provider, Rackspace/AWS. All backup and archival media containing Subscriber Data or Subscriber Confidential Information must be contained in secure, environmentally-controlled storage areas owned, operated, or contracted for by Benchmark Digital. All backup and archival media containing Subscriber Data or Subscriber Confidential Information must be encrypted.

Measures for ensuring events logging

Benchmark Digital application record includes a view history (audit trail history) section, which allows users to view what action was performed, when, and by whom. Users have the ability to select display options and/or filter criteria based on input values, company hierarchy, date ranges etc and create charts for dashboard at-a-glance performance which can be shared with other system users.

All logs are centralized and stored in a Splunk server (local version, not cloud service). Splunk handles page timing reports, SLA tracking, in-depth analysis of web server data, monitoring internal infrastructure. Monthly access audits are performed and HPA audits occur weekly. Event logs are reviewed and audited for outlying traffic and flagged for review immediately. Transactional logs are kept per business and can be utilized for suspicious behavior.

Measures for internal IT and IT security governance and management

Benchmark Digital maintains compliance with applicable laws, applicable standards of the International Standards Organization ISO-27001 (currently under evaluation,), FDA and all other industry standards. Benchmark Digital allows for subscribers to audit (directly or through an agent) the company security program to verify compliance. Audits are conducted at agreed-upon times, during normal business hours, upon reasonable written notice.

Measures for certification/assurance of processes and products

Benchmark Digital software lifecycle includes three separate environments for testing, stage, and production. To facilitate training or demonstration needs, a separate site entity (Demonstration) is established within each subscriber production instance to enable sample data records to be entered. Each Customer-specific release will go through an extensive internal testing process by the Benchmark product development and service delivery teams followed by a screen share review with the team to compare against the project/enhancement specifications and get feedback. All development files and application data are backed up regularly and can be restored as needed. All updates are performed in a separate development, testing, and production lifecycles. All changes are verified and not promoted to the next level until cleared. In production, server-side validation protects against harmful attacks or exploits of code. Each subscribing business will be assigned a dedicated service team. The Benchmark Relationship Leader will be the main point of contact and direct representative on the Benchmark team. This individual will coordinate follow-up on requests/problem reports and other support requests submitted through the Benchmark Help Me! Application and is available for phone/in-person meetings. Additionally, the Relationship Leader will work regularly with the designated Customer Business Administrator and other project managers to determine launch strategies, identify support needs, and to share on-going Benchmark updates. The Relationship Leader will be assisted by the Account Manager to ensure that all customer responses commitments are met. Escalation of issues should be directed through the designated Benchmark Relationship Leader, and further through to the Account Manager and Executive Directors who will be responsible for project oversight, strategic planning, and customer relationship.

Measures for ensuring data minimisation

Benchmark Digital doesn't collect any additional information besides the one previously agreed with data controller under explicit instructions, solely for the purpose of performing its obligations or enforcing its rights under the Agreement, and not for any other purpose.

Measures for ensuring data quality

- Assess legacy system and historical data definition relative to Benchmark module record requirements.
- Establish customer data transfer expectations date range, record types, record detail, etc.
- Define mapping transfer function, limitations and data gaps fill needs and process if applicable (requires inputs from customer IT teams)
- Define legacy system data extraction responsibilities formatting and delivery (requires inputs from customer IT teams)
- Establish execution process, timeline and quality assurance and process for customer review and sign off.

Measures for ensuring limited data retention

All Data is retained in perpetuity. Benchmark Digital can set up differentiated data retention based on customer requirements. Your organization will always be able to access and download all data at will through online export functions. Upon cancelling the contract, data is disposed in accordance with the Benchmark Digital Partners IT and Data Security policy.

Measures for ensuring accountability

Benchmark Digital conducts formal security awareness training for all employees as soon as reasonably practicable after the time of hiring or prior to being appointed to work on Subscriber Data or Subscriber Confidential Information and annually recertified thereafter Data protection/security policies are in place and yearly reviewed (at a minimum) annually or as circumstances arise by the seniormanagement team and IT security personnel.

Benchmark application access is only assigned to appropriate individuals to prevent unauthorized access to confidential and private data within applications. All Benchmark users are required to use have appropriate permissions to access applications, with the exception of open access applications that require an open viewing for all workers based on compliance requisites.

Application Permissions are managed directly by the business. Access granting is only provided in batch upon initiation of the business instances in Benchmark and upon special request by the designated Benchmark Business Administrator.

Measures for allowing data portability and ensuring erasure]

Disposal of Subscriber Data and Subscriber Confidential Information on paper is done in accordance with the Benchmark Digital IT and Data Security policy.

All electronic storage media containing Subscriber Data or Subscriber Confidential

Information is wiped or degaussed for physical destruction or disposal, in a manner meeting forensic industry standards such as the NIST SP800-88 Guidelines for Media Sanitization, prior to departing Subscriber Work Area(s). Benchmark Digital retains commercially reasonable documented evidence of data erasure and destruction for datacenter storage media.

ANNEX III

LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

1. Name: Cloudflare, Inc

Address: 101 Townsend Street, San Francisco, California 94107, United States

Contact person's name, position and contact details: Please use Benchmark Digital Partners Contact. Contact will liaise with Cloudflare as needed to provide the appropriate information.

Description of processing:Cloudflare, Inc. ("Cloudflare") provides content distribution, security, abuse prevention and DNS services for web traffic transmitted to and from the Services. This allows Benchmark Digital Partners to efficiently manage traffic and secure the Services. The primary information Cloudflare has access to is information in and associated with the Benchmark Digital Partners website URL that the End-User is interacting with. All information (including Service Data) contained in web traffic transmitted to and from the Services is transmitted through Cloudflare's systems. Cloudflare also processes a limited amount of Personal Data (specifically Agent and End-User IP addresses, browser and operating system related information) for logging and abuse prevention purposes.

Data Center Locations: https://www.cloudflare.com/network/

2. Name: Amazon Web Services, Inc.

Address: 410 Terry Ave. N., Seattle, WA 98109-5210, United States

Contact person's name, position and contact details: Please use Benchmark Digital Partners Contact. Contact will liaise with AWS as needed to provide the appropriate information.

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): Hosting Provider for Benchmark Digital Partners.

3. Name. Microsoft Corporation, Inc.

Address: 1 Microsoft Way, Redmond, WA 98052, United States

Contact person's name, position and contact details: Please use Benchmark Digital Partners Contact. Contact will liaise with Azure as needed to provide the appropriate information.

Description of the processing: Microsoft Power BI reporting solution, data preparation, data visualization, distribution, and management through development tools and an online platform hosted on Azure clould based environment. Power BI is used to generate reports using customer's data source.