Enlighted Data Processing Addendum

1. Definitions

1.1 "**Agreement**" means the agreement between Enlighted and Company which this DPA is attached to.

1.2 "**Binding Corporate Rules for Processors**" or "**BCR-P**" shall mean binding corporate rules in the meaning of Article 47 GDPR implemented in a group of companies that apply to Personal Data received from a Controller established in the EEA which is not a member of the group and then processed by the group members as Processors and/or Sub-Processors.

1.3 "**Controller**" means the Company and – as the case may be – Further Service Recipients which, alone or jointly with others, determine the purposes and means of the Processing of Personal Data;

1.4 "**Country with an Adequacy Decision**" shall mean a country outside the EEA, where the European Commission has decided that the country ensures an adequate level of protection with respect to Personal Data.

1.5 "**DPA**" shall mean this Data Processing Agreement.

1.6 "**EEA**" shall mean the European Economic Area.

1.7 "**Emergency Replacement**" refers to a short-term replacement of a Sub-Processor which is necessary (i) due to an event outside of Enlighted' reasonable control and (ii) in order to provide the Services without interruptions (such as if the Sub-Processor unexpectedly ceases business, abruptly discontinues services to Enlighted, or breaches its contractual duties owed to Enlighted).

1.8 "**EU Model Contract**" means the Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries pursuant to Commission Decision 2010/87/EU of 5 February 2010 or any successor agreement issued by the European Commission.

1.9 "**Further Service Recipient**" shall mean any third party (such as an affiliated company of Company) which is entitled to receive Services under the terms of the Agreement.

1.10 "**GDPR**" shall mean the General Data Protection Regulation (EU) 2016/679.

1.11 "**Non-EEA Sub-Processor**" shall mean a Sub-Processor Processing Personal Data outside a Country with an Adequacy Decision or accessing Personal Data from outside a Country with an Adequacy Decision.

1.12 "**Personal Data**" has the meaning given to that term in the applicable data protection law and, for the purposes of this DPA, includes only such Personal Data Processed by Enlighted as Company's and/or Further Service Recipient's Processor.

1.13 "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data Processed under the terms of this DPA.

1.14 "**Processor**" means a natural or legal person, public authority, agency or any other body which Processes Personal Data on behalf of a Controller.

1.15 "**Processing**" means any operation or set of operations which is performed upon Personal Data or sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.16 "**Privacy Shield**" means – with regard to Controllers located within the EEA – the European Union / United States Privacy Shield arrangement or – with regard to Controllers located in Switzerland – the Switzerland / United States Privacy Shield arrangement.

1.17 "**Sub-Processor**" shall mean any further Processor engaged in the performance of the Services provided under the terms of this DPA. Sub-Processor shall only mean a subcontractor with access to Personal Data, a subcontractor without access to Personal Data shall not qualify as Sub-Processor in the meaning of this DPA.

1.18 "**Transfer Safeguards**" shall mean (i) an adequacy decision in the meaning of Article 45 GDPR or (ii) appropriate safeguards as required by Article 46 GDPR.

1.19 "**Transfers to Non-EEA Recipients**" shall mean (i) the Processing of Personal Data outside the EEA or a Country with an Adequacy Decision or (ii) any accesses to Personal Data from outside the EEA or a Country with an Adequacy Decision by Enlighted or any of its Sub-Processors.

2. Scope of the DPA and compliance with applicable data protection law

2.1 This DPA serves as written commissioned data processing agreement between Company and Enlighted and applies to services (as further specified in Attachment 1) provided under the Agreement that involve the Processing of Personal Data by Enlighted acting in its role as Processor (each such service hereinafter referred to as "Service"). The DPA describes Company's and Enlighted' data protection related rights and obligations with regard to the Services; all other rights and obligations shall be exclusively governed by the other parts of the Agreement.

2.2 When providing the Services, Enlighted will comply with all data protection laws and regulations directly applicable to Processors. However, Enlighted is not responsible for compliance with any data protection laws or regulations applicable to Company, Further Service Recipients (if any) or Company's industry that are not generally applicable to Processors. Company shall ensure that Enlighted and its Sub-Processors are allowed to provide the Services as described in this DPA.

3. Details of the Processing operations provided by Enlighted

The details of the Processing operations conducted by Enlighted, including the scope, the nature and purpose of the Processing, the types of Personal Data Processed and the categories of affected data subjects, are specified in Attachment 1.

4. Company's instructions and disclosure of customer data

4.1 As Processor, Enlighted will only Process Personal Data upon Company's documented instructions. The Agreement (including this DPA) constitutes Company's complete and final instructions for the Processing of Personal Data by Enlighted as Company's Processor. Any additional or alternate instructions must be agreed between Enlighted and Company in writing and may be subject to additional costs. Enlighted shall inform Company if, in the opinion of Enlighted, an instruction infringes applicable data protection law. Enlighted shall, however, not be obligated to perform any legal examination of Company's instructions.

4.2 Enlighted shall be entitled to disclose or to entitle its Sub-Processors to disclose Personal Data to comply with applicable laws and/or governmental orders. In case of such a request, Enlighted or the Sub-Processor will (i) attempt to redirect such requesting entity to request data directly from Company and may provide Company's basic contact information, and (ii) promptly notify Company and provide a copy of the request, unless Enlighted is prevented from doing so by applicable laws or governmental order.

5. Technical and organizational measures

5.1 Enlighted shall implement the technical and organizational measures described in Attachment 2. Company hereby confirms that the level of security provided is appropriate to the risk inherent with the Processing by Enlighted on behalf of Company.

5.2 Company understands and agrees that the technical and organizational measures are subject to technical progress and development. In that regard, Enlighted shall have the right to implement adequate alternative measures as long as the security level of the measures is maintained.

6. Confidentiality of the processing

Enlighted will ensure that personnel who are involved with the Processing of Personal Data under the DPA have committed themselves to confidentiality.

7. Sub Processors

7.1 Company hereby approves the engagement of Sub-Processors by Enlighted. A current list of Sub-Processors is contained in Attachment 3.

7.2 Enlighted may remove or add new Sub-Processors at any time and inform Company accordingly in advance. The Company may raise objections against such a Sub-Processor within 10 days in which case the parties will try to find an agreement (e.g. termination or different sub-processor). If no objections are raised the Sub-Processors are considered approved.

7.3 Enlighted shall be entitled to perform Emergency Replacements of Sub-Processors. In such case Enlighted shall inform Company of the Emergency Replacement without undue delay and the process as described in Section 7.2 shall apply mutatis mutandis after Company's receipt of the notification.

8. Non EEA and Privacy Shield Certified Sub-Processors

8.1 In case Transfers to Non-EEA Recipients relate to Personal Data originating from a Controller located within the EEA or Switzerland, this Article 8 shall apply and Enlighted shall implement the Transfer Safeguards identified per Sub-Processor in Attachment 3. It is Company's responsibility to assess whether the respective Transfer Safeguard implemented suffices for Company and Further Service Recipients (if any) to comply with applicable data protection law.

8.2 The following shall apply if a Transfer Safeguard is based on the EU Model Contract: Enlighted enters into such EU Model Contract with the relevant Sub-Processor. Each EU Model Contract shall contain the right for Company and Further Service Recipient (if any) located within the EEA or Switzerland to accede to the EU Model Contact. Company hereby accedes to the EU Model Contracts (as a data exporter) with current Sub-Processors and agrees that its approval of future Sub-Processors in accordance with Section 7.2 shall be deemed as declaration of accession to the EU Model Contact with the relevant future Sub-Processor. Furthermore, Company agrees to procure assent from each of its Further Service Recipients (also as data exporters) to accede to such EU Model Contracts. Enlighted hereby waives (also on behalf of the respective Sub-Processor) the need to be notified of the declaration of accession of Company or Further Service Recipients.

8.3 The following shall apply if a Transfer Safeguard is based on the Privacy Shield or Processor Binding Corporate Rules: Enlighted shall contractually bind such Sub-Processor to comply - as the case may be - with the principles of its Privacy Shield certification or its Processor Binding Corporate Rules.

9. Rectification and erasure

Enlighted shall, at its own discretion, either (i) provide Company with the ability to rectify or erase Personal Data via the functionalities of the Services, or (ii) rectify or erase Personal Data as instructed by Company.

10. Personal Data Breach

In the event of any Personal Data Breach, Enlighted shall notify Company of such breach without undue delay after Enlighted becomes aware of it. Enlighted shall (i) reasonably cooperate with Company in the investigation of such event; (ii) provide reasonable support in assisting in Company's security breach notification obligations under applicable data protection law (if applicable); and (iii) initiate respective and reasonable remedy measures.

11. Further notifications and support

11.1 Enlighted shall notify Company without undue delay of (i) complaints or requests of data subjects whose Personal Data are Processed pursuant to this DPA (e.g. regarding the rectification, erasure and restrictions of Processing of Personal Data) or (ii) orders or requests by a competent data protection authority or court which relate to the Processing of Personal Data under this DPA.

11.2 At Company's request, Enlighted shall reasonably support Company in (i) dealing with complaints, requests or orders described in Section 11.1 above (especially in fulfilling Company's obligation to respond to requests for exercising data subject's rights) or (ii) fulfilling any of Company's further obligations as Controller under applicable data protection law (such as the obligation to conduct a data protection impact assessment). Such support shall be compensated by Company on a time and material basis.

12. Audits

12.1 Company shall have the right to audit, by appropriate means - in accordance with Articles 12.2 to 12.4 below – Enlighted' and Sub-Processors' compliance with the data protection obligations hereunder annually (in particular in regard to the technical and organizational measures implemented), unless additional audits are necessary under applicable data protection law; such audit being limited to information and data processing systems that are relevant for the provision of the Services provided to Company.

12.2 Enlighted and Sub-Processors may use (internal or external) auditors to perform audits to verify compliance with the data protection obligations hereunder. In such case each audit will result in the generation of an audit report (e.g. Service Organization Controls 1, Type1 or Type 2 reports and Service Organization Controls 2, Type1 or Type 2 reports). Where a control standard and framework implemented by Enlighted or our Sub-Processors provides for audits, such audit will be performed according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework. Upon Company's request, Enlighted shall provide such relevant Audit Reports for the Services concerned.

12.3 Company agrees that these audit reports and corresponding information provided by Enlighted (together "Audit Reports") shall first be used to address Company's audit rights under this DPA. In case Company can demonstrate that the Audit Reports provided are not reasonably sufficient to allow Company or a Further Service Recipients to comply with applicable audit requirements and obligations under applicable data protection law, Company shall specify the further information, documentation or support required. Enlighted shall render such information, documentation or support within a reasonable period of time at Company's expense.

12.4 The Audit Reports and any further information and documentation provided during an audit shall constitute Confidential Information and may only be provided to Further Service Recipients pursuant to confidentiality obligations substantially equivalent to the confidentiality obligations contained elsewhere in the Agreement. In case audits relate to Sub-Processors, Company and Further Service Recipients may be required to enter into non-disclosure agreements directly with the respective Sub- Processor before issuing Audit Reports to Company or Further Service Recipients.

13. Term and Termination

This DPA shall have the same term as the Agreement. Upon termination of the DPA, unless otherwise agreed between the Parties, Enlighted shall erase all Personal Data made available to Enlighted or obtained or generated by Enlighted on behalf of Company in connection with the Services. The erasure shall be confirmed by Enlighted in writing upon request.

Please sign and return the enclosed copy of this Addendum as instructed to acknowledge the supplementation of these terms to the Agreement.

COMPANY

Company name (Required): _____
Signature (Required): _____
Name (Required): _____
Title (Optional): _____
Date (Required): _____
EU Representative (Required only where applicable): _____
Contact details: _____
Data Protection Officer (Required only where applicable): _____
Contact details: _____

ENLIGHTED

Data Protection Point of Contact: Mandeep Singh
Contact Details: privacy@enlightedinc.com
Signature: _____
Name: _Mandeep Singh_____
Title: __VP, Technical Operations_
Date: __Aug, 06, 2019_____

Attachment 1: Description of the data processing activities

This attachment describes the general data processing activities regarding services offered by Enlighted for the Product as well as the affected persons and the categories of the processed personal data.

Product	**Service**	**Explanation**
Enlighted Where	Data Storage	Administrators and Users data such as Organization Name, First Name, Last Name, Email, Address and Phone numbers are stored in the Enlighted database on a cloud environment.
	Software support	During software support there is Company data visible which may contain personal data (e. g. personal names of employees). Further Enlighted is able to help Company to delete data.
Categories of affected persons • Persons who are using the product (employee of Company, employee of third party etc.)		
Category of data • Business contacts (Mail-address, Phone number) • Personal master data (name, username, office address, validity, user rights, employee number, access rights etc.)		

Attachment 2: Technical and organizational measures

(Pursuant to Art. 32 General Data Protection Regulation ("GDPR"))

1. Physical Access Control

The following measures are implemented to protect against unauthorized physical access to premises, buildings or rooms where data processing systems are located which process and/or use Personal Data:

a) Physical components of the data center facilities, servers, networking equipment, and host software are housed in nondescript facilities.
b) Physical barrier controls are used to prevent unauthorized entrance to these facilities both at the perimeter (e.g., fencing, walls) and at building access points.
c) Physical access points to server locations are managed by electronic access control devices and are secured with intrusion detection devices that sound alarms if the door is forced open or held open.
d) Establishing access authorizations for employees and third parties, including the respective documentation.
e) All visitors are required to present identification and are signed in.
f) Use of video cameras (CCTV) to monitor individual physical access to data center facilities.
g) Data centers utilize security guards 24x7, who are stationed in and around the building.

2. System Access Control

The following measures are implemented to protect against the unauthorized access to and use of data processing systems used to provide the digital services:

a) User and administrator access to the data center facilities, servers, networking equipment, and host software is based on a role-based access rights model. A unique ID is assigned to ensure proper user-authentication management for users and administrators on all system components.
b) The concept of least privilege is employed, allowing only the necessary access for users to accomplish their job function. When user accounts are created, user accounts are created to have minimal access. Access above these least privileges requires appropriate authorization.
c) System Administrator access privileges are reviewed on regular basis by appropriate personnel.
d) Access to systems is revoked within a reasonable timeframe of the employee record being terminated (deactivated).
e) First time passwords/passphrases are set to a unique value and changed immediately after first use.
f) User passwords/passphrases are changed periodically and only allow complex passwords.
g) Time stamped logging of security relevant actions is in place.
h) Automatic time-out of user terminal if left idle, with user identification and password required to reopen.
i) Assets (e.g. laptops) are configured with anti-virus software that includes e-mail filtering and malware detection.
j) Firewall devices are configured to restrict access to the computing environment and enforce boundaries of computing clusters.
k) Firewall policies (configuration files) are pushed to firewall devices on regular basis.

3. Data Access Control

The following measures are implemented to control that persons entitled to use data processing systems gain access only to the Personal Data when they have a right to access, and Personal Data is not read, copied, modified or removed without authorization in the course of processing, use and storage.

a) User and administrator access to the data center facilities, servers, networking equipment, and host software is based on a role-based access rights model. A unique ID is assigned to ensure proper user-authentication management for users and administrators on all system components.
b) The concept of least privilege is employed, allowing only the necessary access for users to accomplish their job function. When user accounts are created, user accounts are created to have minimal access. Access above these least privileges requires appropriate authorization.
c) System administrator access privileges are reviewed on regular basis by appropriate personnel.
d) Time stamped logging of access to and modification of Personal Data is in place.
e) An incident response plan is in place to address the following at time of incident:
    - Roles, responsibilities, and communication and contact strategies in the event of a compromise.
    - Specific incident response procedures.
    - Coverage and responses of all critical system components

4. Data Transmission Control

The following measures are implemented to control that Personal Data is not read, copied, modified or removed without authorization during transfer:

a) Prevention of unauthorized copying: The measures taken to prevent unauthorized copying of the physical storage infrastructure as such (e.g. copying your data by transferring them to an external storage medium as a hard drive) are included in the measures described above.
b) Use of role-based access rights model: described above.
c) Firewall policies: described above
d) Implement an incident response plan: described above.
e) Storage Device Decommissioning: When a storage device has reached the end of its useful life, procedures implemented include a decommissioning process that is designed to prevent Company data from being exposed to unauthorized individuals. All decommissioned magnetic storage devices are degaussed and physically destroyed in accordance with industry-standard practices and applicable data protection law.
f) Secure Access Points: there are only a limited number of secure access points to the cloud), which allow you to establish a secure communication session with your storage or compute instances within the Services.
g) Connections to the network by personnel: personnel connect to the network using secure authentication that restricts access to network devices and other cloud components.

5. Data Input Control

The following measures are implemented to retrospectively examine and establish whether and by whom Personal Data have been entered, modified or removed from data processing systems used to provide the digital services:

a) Logging User Activity: developers and administrators who need to access to our systems in order to maintain them must explicitly request access. Approved personnel connect to the network using secure authentication that restricts access to network devices and other cloud components, logging all relevant activity for security review.

6. Order Control

The following measures are implemented in order to ensure that Personal Data which are processed on your behalf can only be processed in compliance with your instructions:

a) Internal communication: various methods of internal communication are implemented at a global level to help employees understand their individual roles and responsibilities and to communicate significant events in a timely manner. These methods include orientation and

training programs for newly hired employees and regular management meetings for updates on business performance and other matters.

b) Corporate Segregation: Logically, the production network is segregated from the corporate network by means of a complex set of network security / segregation devices. Developers and administrators on the corporate network who need to access in order to maintain them must explicitly request access. Approved personnel then connect to the network through secure means.

c) Robust Compliance Program: The IT infrastructure is designed and managed in alignment with security best practices and certain IT security standards, such as SOC2 and/or ISO 27001.

d) Policies and Security Awareness Training: We and our Subprocessors maintain and provide periodic security awareness training to all information system users. Policies and procedures have been established based upon data security and data protection requirements.

7. Availability Control

The following measures are implemented to protect Personal Data against accidental or unauthorized destruction or loss.

a) Fire Detection and Suppression: Automatic fire detection and suppression equipment has been installed with our data centers. The fire detection system utilizes smoke detection sensors in all data center environments, mechanical and electrical infrastructure spaces, chiller rooms and generator equipment rooms.

b) Redundant Power Systems: The data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and seven days a week. Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. Data centers use generators to provide back-up power for the entire facility.

c) Climate and Temperature Control: Personnel and systems monitor and control temperature and humidity at appropriate levels at data centers.

d) Preventative maintenance: Preventative maintenance is performed to maintain the continued operability of the data center equipment.

8. Data Separation Control

The following measures are implemented to control that Personal Data collected for different purposes can be processed separately:

a) Multi-tenant environment: The Platform is a virtualized, multi-tenant environment. Security management processes and security controls designed to isolate each Company from others are implemented. Systems are designed to prevent Company and other customers from accessing physical hosts or instances not assigned to them by filtering through the virtualization software.

b) Corporate Segregation: described above.

Attachment 3: List of approved Sub-Processors

This attachment lists the Sub-Processors engaged by Enlighted when providing Services to the Company

Sub-Processor name	Sub-Processor Country	Service provided by Sub-Processor	Transfer Safeguards implemented by Sub-Processor	
Google LLC, 1600 Amphitheatre Pkwy, Mountain View, California 94043 (incl. other entities: https://cloud.google.com /terms/subprocessors)	USA	Hosting of data	☐	Not applicable, Sub-Processor located within the EEA / a Country with An Adequacy Decision
			☐	EU Model Contract
			☒	Privacy Shield
			☐	BCR-P