PINEWOOD TECHNOLOGIES DATA PROCESSING ADDENDUM

PARTIES

This Data Processing Addendum ("DPA") is an agreement between the Pinewood group contracting legal entity as defined on the Order Form ("Pinewood," "we," "us," or "our") and you or the entity you represent ("Customer", "you" or "your"). This DPA supplements the Pinewood Standard Terms & Conditions as updated from time to time between Customer and Pinewood, or other agreement between Customer and Pinewood governing Customer's use of the Software as a Service (the "Agreement") when it applies to your use of the Services to process Customer Data. Unless otherwise defined in this DPA or in the Agreement, all capitalized terms used in this DPA will have the meanings given to them in Section 1 of this DPA.

BACKGROUND

A. The Data Controller and the Data Processor have entered into an agreement separate to this DPA, for the Data Processor to deliver goods and/or, to provide services as the case may be to the Data Controller which involves the processing of Personal Data of or relating to certain individuals by the Data Processor on behalf of the Data Controller.

B. The parties agree that the Data Processor shall process certain Personal Data provided to it by the Data Controller in accordance with the terms and conditions set out in this DPA.

AGREED TERMS

1. Interpretation

1.1. The definitions and rules of interpretation in this clause apply in this DPA.

Affiliate includes in relation to either party each and any subsidiary or holding company of that party and each and any subsidiary of a holding company of that party

Authorized Recipient has the meaning given to it in clause 13.3(a)

Business Day means Monday to Friday, excluding any public holidays in the country of operation

Confidential Information means all information, data or materials received from the other (including, without limitation, drawings, sketches, photographs, vehicle prototypes, models, computer software, ideas, design, know-how, formulae, processes, copyrights, inventions, techniques, new product details, business plans and such other matters as may reasonably be regarded by either party as confidential and any copies thereof in any media whatsoever) shall be kept strictly confidential at all times.

Data Controller/Controller has the meaning set out in the Data Protection Legislation

Data Protection Legislation means applicable legislation relating to data protection and privacy which applies to either Party or all Parties to this DPA, including without limitation the Data Protection Act 2018, The General Data Protection Regulation 2016/679/EC ("GDPR"), any national implementation of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector as well as, in respect of the United Kingdom, any applicable national legislation that replaces or converts into domestic law the GDPR or any other law relating to data and privacy as a consequence of the United Kingdom leaving the European Union in each case as amended, repealed, consolidated or replaced from time to time, all federal and state Privacy laws in the United States of America including, but not limited to the California Consumer Privacy Act of 2018 (CCPA) and the Children's Online Privacy Protection Act, 15 U.S.C. ss. 6501 et seq., The Protection of Personal Information Act 4 of 2013 (POPIA) in South Africa, The Act on the Protection of Personal Information ("APPI") in Japan, and the Protection of Personal Data Protection ("PDPL") in the United Arab Emirates;

Data Protection Officer means a designated person appointed by each party with the same position and tasks to inform and advise, and to monitor compliance with the requirements of each respective party as set out under the Data Protection Legislation

Data Privacy Notice means a notification given to the Data Subject concerned in relation to the processing of the Data Subject's Personal Data in accordance with the Data Protection Legislation

Data Subject an individual who is the subject of Personal Data

DPIA means a data protection impact assessment or privacy impact assessment

Group means a party and its Affiliates

Insolvency Event means, in respect of a party, the occurrence of any of the following events:

a) it is unable to pay its debts as they fall due;

b) it ceases, or threatens to cease, to carry on its business;

c) any step is taken with a view to the appointment of a liquidator, receiver, administrator or administrative receiver to it or over any part of its undertaking or assets;

d) it passes a resolution for its winding up (otherwise than for the purpose of a bona fide scheme of solvent amalgamation or reconstruction where the resulting entity assumes all of its liabilities);

e) a court of competent jurisdiction makes an administration order or liquidation order or similar order in relation to it, or any step is taken with a view to obtaining such an order;

f) it enters into, or proposes, any voluntary arrangement with its creditors; or

g) any event analogous to those set out in paragraphs (a) to (f) above occurs in any jurisdiction in relation to it.

Personal Data shall have the meaning set out in the Data Protection Legislation and more particularly described in Schedule 1 and to include any other data processed by the Data Processor for the purposes of this DPA

Processing and **Process** have the meaning set out in the Data Protection Legislation.

Data Processor/Processor has the meaning set out in the Data Protection Legislation

Regulator means any person or professional body or law enforcement agency anywhere in the world having regulatory, supervisory or governmental authority (whether under a statutory scheme or otherwise) over all or any part of the businesses of each of the parties to this DPA

Recipient has the meaning given to it in clause 13.1(a)

1.2. The headings in this DPA do not affect its interpretation. Except where the context otherwise requires, references to clauses and schedules are to clauses and schedules of this DPA.

1.3. Unless the context otherwise requires:

a) references to the Data Controller include their permitted successors and assigns;

b) references to statutory provisions include those statutory provisions as amended or re-enacted;

c) a reference to one gender includes a reference to the other genders; and

d) references to "including" or "includes" shall be deemed to have the words "without limitation" inserted after them.

1.4. In the case of conflict or ambiguity between any provision contained in the body of this DPA and any provision contained in the schedules, the provision in the body of this DPA shall take precedence.

1.5. Words in the singular include the plural and those in the plural include the singular.

1.6. A **person** includes a natural person, corporate or unincorporated body (whether or not having separate legal personality) and that person's personal representatives, successors or permitted assigns.

2. Processing characterization and notifications

2.1. Customer and the Data Processor acknowledge that for the purposes of the Data Protection Legislation, Customer is the Controller and Pinewood Technologies PLC is the Processor in respect of the Personal Data processed by the Data Processor. The Data Controller assigns the Data Processor with the Processing of Personal Data on behalf of the Data Controller within the meaning of the Data Protection Legislation.

3. The Data Processor's obligations

3.1. The Data Processor shall adhere to the instructions of a controller and shall assist the controller in meeting or complying with the controller's duties, including the following:

a) Assisting the controller in responding to consumer rights requests submitted, by using appropriate technical and organizational measures, as reasonably practicable, taking into account the nature of processing and the information available to the processor;

b) Assisting the controller with regard to complying with the requirement relating to the security of processing personal data and to the notification of a breach of security of the processor's system, taking into account the nature of processing and the information available to the processor;

c) Assist the controller in complying with obligations relating to security of processing, Personal Data breach notification and DPIAs.

d) Maintain adequate records of all processing of the Personal Data in the form of a Data Processing Register, including of the training of the Data Processor's personnel with regard to the Data Protection Legislation.

4. Controls and other responsibilities of the Data Processor

4.1. The Data Processor shall;

a) Appoint a Data Protection Officer whose name and contact details are shared with the Data Controller. Any change in the Data Protection Officer's contact details shall be supplied to the Data Controller.

b) The Data Processor shall maintain confidentiality and all persons who have access to Personal Data belonging to the Data Controller under the terms of this DPA undertake to maintain confidentiality and shall be informed of any special data protection requirements arising from the Agreement, and the limitation of use to specific purposes as instructed.

c) The Data Processor shall implement and maintain all technical and organizational security measures required for the Agreement according to the Data Protection Legislation in addition to the measures specified in Schedule 2 to the DPA.

d) The Data Processor shall immediately notify the Data Controller of any activities and measures including but not limited to monitoring activities undertaken by a Regulator.

e) The Data Processor shall give all reasonable assistance to the Data Controller for the fulfilment of the Data Controller's accountability and documentation obligations arising under the Data Protection Legislation.

f) The Data Processor shall assist the Data Controller, by implementing appropriate technical and organizational security measures, to enable the Data Controller to fulfil its obligation to respond to requests for exercising the Data Subject's rights under the Data Protection Legislation.

g) The Data Processor shall assist the Data Controller to ensure compliance with the obligations pursuant to the Data Protection Legislation including without limitation, security, breach notification, data protection assessments and consulting with supervisory authorities, taking into account the nature of Processing and the information available to Data Processor.

h) The Data Processor shall take reasonable steps to ensure the reliability of all its employees who have access to the Personal Data and shall ensure that only those of the Data Processor's personnel who need to have access to the Personal Data are granted access to such data and only for the purposes envisaged under this DPA and all of the Data Processor's personnel required to access the Personal Data are adequately trained in all relevant Data Protection Legislations, and are under the same confidentiality obligations as the Data Processor.

i) The Data Processor shall assist Data Controller in responding to consumer rights requests, including access, deletion, correction, opt-out of sale/sharing, and opt-out of automated decision-making. Responses must be provided within the statutory timelines and recorded.

j) The Data Processor warrants that it has power to execute this DPA and that once executed it will be binding upon it.

5. The Data Controller's obligations

5.1. The Data Controller shall:

a) Limit the collection of personal data to data that is adequate, relevant, and reasonably necessary in relation to the purposes for which it is processed, as disclosed to the consumer;

b) For purposes of protecting the confidentiality, integrity, and accessibility of personal data, establish, implement, and maintain reasonable administrative, technical, and

physical data security practices appropriate to the volume and nature of the personal data at issue;

c) Provide the Data Processor with the Personal Data, Data Protection Notice and such instructions and other information as are reasonably required to perform the services that the Data Processor has been engaged to do;

d) Ensure that any instructions will comply with Applicable Laws;

e) Warrants that it has power to execute this DPA and that once executed it will be binding on it; and

f) Appoint a Data Protection Officer whose name and contact details are shared with the Data Processor. Any change in the Data Protection Officer's contact details shall be supplied to the Data Processor.

5.2. The Data Controller may not do any of the following:

a) Except as otherwise provided by this part, process personal data for a purpose that is neither reasonably necessary nor compatible with the purpose for which the personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent.

b) Process personal data in violation of state or federal laws that prohibit unlawful discrimination against consumers.

c) Discriminate against a consumer for exercising any of the consumer rights contained in this part, including by denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods or services to the consumer. A controller may offer financial incentives, including payments to consumers as compensation, for processing of personal data if the consumer gives the controller prior consent that clearly describes the material terms of the financial incentive program and provided that such incentive practices are not unjust, unreasonable, coercive, or usurious in nature. The consent may be revoked by the consumer at any time.

d) Process the sensitive data of a consumer without obtaining the consumer's consent, or, in the case of processing the sensitive data of a known child, without processing that data with the affirmative authorization for such processing by a known child as defined in the relevant Data Protection Legislations.

6. Notification of Infringements

6.1. The Data Processor and the Data Controller shall without undue delay notify each other where errors, irregularities or suspected infringements of provisions relating to the

protection of Personal Data occur. The Parties agree to take all reasonable measures in order to remedy infringements immediately.

6.2. The Data Processor shall without undue delay notify the Data Controller in all cases where the Data Processor or persons employed by them infringe provisions relating to the protection of Personal Data belonging to the Data Controller or any other stipulations set out in the Agreement.

6.3. The parties are aware that the Data Protection Legislation imposes a duty to inform in the event of a data protection infringement or breach. Such incidents (including but not limited to any loss, unlawful disclosure or unlawful access to Personal Data) shall therefore be notified to the Data Controller without undue delay. This also applies to serious operational faults or where there is any suspicion of an infringement of provisions relating to the protection of Personal Data or other irregularities in the handling of Personal Data belonging to the Data Controller. Notification shall include the nature of the infringement, categories of data affected, mitigation measures, and contact information. Upon consultation with the Data Controller, the Data Processor shall take appropriate measures to secure the data and limit any possible detrimental effect on the Data Subjects. Where obligations are imposed on the Data Controller under the Data Protection Legislation the Data Processor shall assist in complying with them.

6.4. The Data Processor shall provide the Data Controller with all reasonable co-operation and assistance in relation to any complaint or request made in respect of any Personal Data at the Data Processor's cost except where the Data Controller is in breach of this DPA, including by:

a) providing the Data Controller with details of the complaint or request;

b) complying with a subject access request within the relevant timescales set out in the Data Protection Legislation and otherwise in accordance with the Data Controller's instructions; and

c) providing the Data Controller within the timescales reasonably required by the Data Controller (to comply with the Data Protection Legislation) with any Personal Data it holds on behalf of the Data Controller in relation to a Data Subject in accordance with the rights of the Data Subject to be provided in an electronic format together with details of how long the data is stored for and, where applicable, details of any data exports outside the originating jurisdiction and the safeguards deployed.

7. Sub-processing

7.1. **Authorized Sub-processors**. Customer agrees that Pinewood may use sub-processors to fulfil its contractual obligations under this DPA or to provide certain services on its

behalf. The Pinewood Trust Center website (currently posted at https://app.eu.vanta.com/pinewood.ai/trust/sewc6f0fw0om7l4yusx27/subprocessors) lists sub-processors that are currently engaged by Pinewood to carry out processing activities on Customer Data on behalf of Customer. At least 30 days before Pinewood engages any new sub-processor to carry out processing activities on Customer Data on behalf of Customer, Pinewood will update the applicable website. Customer consents to Pinewood's use of sub-processors as described in this Section. Except as set forth in this Section, or as Customer may otherwise authorize, Pinewood will not permit any sub-processor to carry out processing activities on Customer Data on behalf of Customer.

7.2. Sub-processor Obligations. Where Pinewood authorizes any sub-processor as described in Section 7.1:

a) Pinewood will restrict the sub-processor's access to Customer Data only to what is necessary to maintain the Services or to provide the Services to Customer and any End Users in accordance with the Documentation and Pinewood will prohibit the sub-processor from accessing Customer Data for any other purpose;

b) Pinewood will enter into a written agreement with the sub-processor and, to the extent that the sub-processor is performing the same data processing services that are being provided by Pinewood under this DPA, Pinewood will impose on the sub-processor the same contractual obligations that Pinewood has under this DPA;

c) To safeguard the protection and security of the Data Controller's Personal Data the Data Processor shall nevertheless conclude adequate and lawful contractual agreements and undertake regular monitoring activities, even where ancillary services are commissioned from third parties.

d) Pinewood will remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the sub-processors that cause Pinewood to breach any of Pinewood's obligations under this DPA.

8. Authority of the Data Controller to issue instructions

8.1. The Data Processor shall at all times be bound by the Data Controller`s instructions relating to the execution of this DPA and the Processing of Personal Data belonging to the Data Controller. The Data Controller retains a general right of instruction as to the nature, scope and method of data Processing, which may be supplemented with individual instructions. The Data Processor may only pass on information to third parties or to the Data Subject with the prior written consent of the Data Controller.

8.2. The Data Processor must not use the data for any other purpose than the execution of the Agreement and is not permitted to disclose the data to third parties. If the Data Processor is legally obliged to disclose any Personal Data, the Data Processor will immediately inform the Data Controller.

8.3. No copies or duplicates may be produced without the knowledge of the Data Controller. This does not apply to backup copies or to the readout of log files etc. where these are required to assure proper data Processing. The Data Processor shall inform the Data Controller immediately and prior to any Processing if the Data Processor believes that an instruction of the Data Controller constitutes an infringement of the Data Protection Legislation. The Data Processor then can postpone the execution of the relevant instruction until it is confirmed or changed by the Data Controller.

9. Audit Rights of the Controller

9.1. The Data Controller may carry out audits on the Data Processor's business premises before the start of the Processing and at reasonable intervals thereafter in order to verify compliance of the technical and organizational security measures implemented by the Data Processor to comply with the terms of this DPA, or appoint auditors to do so. Audits shall not take place more frequently than once a year unless there is a regulatory investigation. The parties shall cooperate in order to agree upon reasonable terms and conditions for such audits. As a first step, upon request by the Data Controller, the Data Processor shall provide the Data Controller with evidence of its implementation of the technical and organizational security measures pursuant to this DPA and the Data Protection Legislation.

9.2. For on-site audits, the Data Controller shall respect the operational activities and processes of the Data Processor and provide reasonable prior notice of audits at least 24 hours in advance.

9.3. The Data Processor undertakes at all times to assist the Data Controller in the execution of the audits.

9.4. The Data Processor undertakes upon request to provide the Data Controller with all the information required to meet the requirements of the Data Protection Legislation and the audit rights referred to in this DPA relating to the Processing of Personal Data, and make the necessary documentation available.

9.5. The Parties shall bear their own costs unless the audit reveals material non-compliance.

10. Transfers of Personal Data

10.1. Any transfer of data to a third country outside of the originating jurisdiction requires:

a) that it is subject to compliance with the Data Protection Legislation; and

b) the parties to enter into Standard Contractual Clauses or any equivalent replacement clauses which are issued as standard contractual clauses by the competent Regulator, a government department or any other similar body authorized to issue such clauses; and

c) such other additional safeguards as required by a Regulator, a government department, any other similar body and/or by Data Protection Legislation regulating such transfers.

11. Correction, Deletion and Return of Personal Data

11.1. The Data Processor may only correct, delete or block Personal Data Processed on behalf of the Data Controller when instructed to do so by the Data Controller. If a Data Subject applies directly to the Data Processor for correction or deletion of his/her Personal Data, the Data Processor shall forward such request to the Data Controller without delay.

11.2. Upon completion of the contractual work or when requested by the Data Controller, the Data Processor shall return to the Data Controller all Personal Data in his possession and all work products and data produced in connection with the Agreement, or irrevocably delete or destroy them in compliance with the Data Protection Legislation with the prior consent of the Data Controller. The deletion log(s) or certificate(s) shall be presented upon request.

11.3. Documentation intended as proof of proper data Processing shall be kept by the Data Processor beyond the end of the Agreement in accordance with relevant retention periods. The Data Processor shall, upon request of the Data Controller, hand such documentation over to the Data Controller after expiry of the Agreement.

11.4. The Data Processor shall maintain confidentiality also after the expiration of this DPA relating to all Personal Data or other information from the Data Controller that came to his attention during the execution of this DPA.

12. Warranties, Liability and Indemnification

12.1. Each party warrants to the other that it will process the Personal Data in compliance with all laws, enactments, regulations, orders, standards and other similar instruments applicable to it.

12.2. Each Party's aggregate liability under this DPA shall be limited to 100% of the total Fees paid pursuant to the commercial agreement to which this DPA relates, excluding breaches of confidentiality, data security obligations, or violation of privacy laws.

12.3. The Data Processor shall not be liable for any special, indirect or consequential loss, costs, damages, charges or expenses however arising under or in connection with this DPA.

12.4. The Data Processor shall indemnify Data Controller for third-party claims arising from Data Processor's violation of applicable privacy laws or this DPA.

12.5. Nothing in this DPA excludes the liability of the Data Processor: for death or personal injury caused by the Data Processor's negligence; for fraud or fraudulent misrepresentation; or for any other liability which cannot be limited or excluded by applicable law.

13. Confidentiality

Obligation of confidence

13.1. Subject to Clause 13.2:

a) each party undertakes to keep confidential and secure all Confidential Information given by or made available by one party to the Agreement (Disclosing party) to the other party (Recipient) or otherwise obtained, developed or created by the Recipient relating to the Disclosing party or any affiliate of either party; and

b) the Recipient shall use the Confidential Information solely in connection with the performance of its obligations or exercise of its rights under the Agreement and not for its own benefit or for the benefit of any third party.

Excluded Categories of information

13.2 The restrictions on use or disclosure of information described in clause 13.1 above do not extend to any information which:

(a) is or becomes generally available to the public other than as a result of a breach of an obligation under this clause; or

(b) is acquired from a third party who owes no obligation of confidence in respect of the information; or

(c) is or has been independently developed by the Recipient or was in the Recipient's lawful possession prior to receipt from the Disclosing party.

Authorized Recipients

13.3 The Recipient may also disclose the Confidential Information:

a) to the Recipient's members, directors, officers, employees, consultants, agents, advisers, contractors, subcontractors and Affiliates to whom disclosure of the Confidential Information is required for the performance of the Recipient's obligations or the exercise of its rights under the Agreement and then only to the extent necessary to perform such obligations or exercise such rights (together the Authorized Recipients); or

b) pursuant to a binding request from any government or regulatory authority or as may be required by law or pursuant to a court order provided that, to the extent

permitted by law, the Recipient gives prompt written notice of the request for disclosure to the Disclosing party, where practicable before it occurs, so that the Disclosing party may have an opportunity to prevent the disclosure through appropriate legal means.

13.4 Before disclosing Confidential Information to an Authorized Recipient, the Disclosing party shall procure that such Authorized Recipient has entered into confidentiality undertakings no less onerous than those contained in this clause and the Recipient shall remain fully liable to the Disclosing party for any breach of the terms of the Agreement by the Authorized Recipient.

General

13.5 Each party shall keep confidential and secure all copies of the Confidential Information that it holds or may hold.

13.6 This clause shall survive the termination or expiry of the Agreement howsoever arising and shall continue in force indefinitely.

13.7 The parties agree that damages may not be an adequate remedy for breach of this clause and (to the extent permitted by the court) that the party not in breach shall be entitled to seek an injunction or specific performance in respect of such breach.

13.8 Upon termination of the Agreement, the Disclosing party shall be entitled to require the Recipient to return or destroy all Confidential Information upon demand, save that the Data Processor shall be entitled to keep one copy of all Confidential Information provided to it by the Data Controller for record keeping purposes.

14 Miscellaneous

Waiver

14.1 No failure or delay by a party to exercise any right or remedy provided under this DPA or by law shall constitute a waiver of that or any other right or remedy, nor shall it preclude or restrict the further exercise of that or any other right or remedy. No single or partial exercise of such right or remedy shall preclude or restrict the further exercise of that or any other right or remedy.

Remedies cumulative

14.2 Except as expressly provided in this DPA, the rights and remedies provided under this DPA are in addition to, and not exclusive of, any rights or remedies provided by law.

Entire Agreement

14.3 This DPA, including the Schedules to this DPA contain the whole Agreement between the parties relating to the subject matter hereof and supersede all prior Agreements,

arrangements and understandings between the parties relating to that subject matter.

14.4 Each party acknowledges that, in entering into this DPA, it does not rely on any statement, representation, assurance or warranty (whether it was made negligently or innocently) of any person (whether a party to this DPA or not) (Representation) other than as expressly set out in this DPA.

14.5 Each party agrees that the only rights and remedies available to it arising out of or in connection with a Representation shall be for breach of contract.

Variation

14.6 No variation of this DPA shall be effective unless it is in writing and signed by the parties (or their authorized representatives).

Severance

14.7 If any court or competent authority finds that any provision of this DPA (or part of any provision) is invalid, illegal or unenforceable, that provision or part-provision shall, to the extent required, be deemed to be deleted, and the validity and enforceability of the other provisions of this DPA shall not be affected.

Counterparts

14.8 This DPA may be executed in any number of counterparts, each of which when executed and delivered shall constitute an original of this DPA, but all the counterparts shall together constitute the same Agreement.

Third-part rights

14.9 A person who is not a party to this DPA shall not have any rights to enforce any term of this DPA, but this does not affect any right or remedy of a third party which exists.

Assignment and subcontracting

14.10 Subject to clause 14.10, neither party may assign, novate, sub-contract or otherwise dispose of the Agreement or any part of it without the prior written consent of the other party.

14.11 The Data Processor may assign all of its rights or transfer all of its obligations under the Agreement, to any company within the Data Processor’s Group or any person which acquires the whole or substantially the whole of the business to which this DPA relates.

14.12 Subject to the provisions of clause 6, the Data Processor may authorize a third party to process the Personal Data (sub-contractor), provided that the sub-contractor's contract:

a. is on terms which are substantially the same as those set out in this DPA; and

b. terminates automatically on termination of this DPA for any reason.

No partnership or agency

14.13 Nothing in this DPA is intended to, or shall be deemed to, establish any partnership or joint venture between any of the parties, constitute any party the agent of another party, nor authorize any party to make or enter into any commitments for or on behalf of any other party.

Notices

14.14 Any notice or other communication required to be given under this DPA shall be in writing and shall be delivered personally, sent by recorded delivery, registered post or by commercial courier, or by electronic mail to each party required to receive the notice as set out below:

a) Data Processor:

Postal Address: Data Protection Officer, 2960 Trident Court, Solihull Parkway, Birmingham Business Park, Birmingham, B37 7YN United Kingdom

Email: dataprotection@pinewood.ai

b) Data Controller: the Customer as detailed in the Order Form or Master Service Agreement.

or as otherwise specified by the relevant party by notice in writing to each other party.

14.15 Any notice or other communication shall be deemed to have been duly received:

a) if delivered personally, when left at the address and for the contact referred to in this clause;

b) if sent by recorded delivery or registered post, at 9.00 am on the second Business Day after posting; or

c) if delivered by commercial courier, on the date and at the time that the courier's delivery receipt is signed.

15 Dispute resolution

15.1 If there are any grounds for dispute refer to the Agreement terms and conditions.

16 Governing law and jurisdiction

16.1 This DPA and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by the laws as stated in the Agreement.

16.2 The parties irrevocably agree that the courts located in each Pinewood contracting legal entity region shall have exclusive jurisdiction to settle any dispute or claim that

arises out of or in connection with this DPA or its subject matter or formation (including non-contractual disputes or claims).

SCHEDULE 1 – DATA INVENTORY

1. **The purpose of the Data Processor's processing of personal data on behalf of the Data Controller is:**

   The Data Processor processes personal data on behalf of the Data Controller for the purpose of providing the services agreed between the Parties to the Agreement stated in the Agreement.

2. **The Data Processor's processing of personal data on behalf of the Controller shall mainly concern (the nature of the processing):**

   The nature of the processing carried out in accordance with the Agreement and in compliance with the DPA will include:

   - Hosting
   - Storage of Data
   - Backup
   - User Support

3. **The processing includes the following types of personal data about the data subjects:**

   The processing will include the following categories of personal data about the data subjects:

   - Identifiers (e.g., name, postal address, email address)
   - Commercial information (e.g., transaction history)
   - Internet or network activity (e.g., IP address, log data)
   - Geolocation data
   - Professional or employment-related information

4. **The processing includes the following categories of data subjects:**

   The categories of data subjects are the identified or identifiable natural persons whose personal data is processed under the DPA. Personal data concerning the following categories of data subjects is processed under the DPA:

   - The Data Controller’s employees
   - The Data Controller’s customers

SCHEDULE 2 – TECHNICAL AND ORGANIZATIONAL MEASURES

Organizational security

- The Data Processor has a documented information security policy that addresses how information security is anchored and implemented in the Data Processor's organization.
- The Data Processor maintains and enforces policies for the secure handling of information and for the purpose of ensuring that personal data is processed in accordance with applicable law. The Data Processor will take appropriate steps to ensure that such policies are known to all employees by conducting regular training.
- The Data Processor will ensure that third-party service providers comply with a minimum set of controls prescribed by the Data Processor and are subject to confidentiality obligations before they are commissioned.
- The Data Processor regularly checks third-party services and Sub-processors based on the risk of their processing of personal data.
- Taking into account the current technological level, the implementation costs and the nature, scope, context and purpose of the processing in question, the Data Processor will implement and comply with the principles of data protection through design throughout all phases of the information's and system's life cycle.

Physical security

- Locations, including data centers, offices and off-site storage facilities, or locations from which the Data Controller's information can potentially be accessed, have appropriate physical security controls to protect against unauthorized access.
- The Data Processor will ensure the secure disposal of information, media, equipment and paper in accordance with recognized industry standards.

System and network security

- Networks and devices on which personal data is processed are protected against unauthorized access or infiltration, both internally and externally.
- Network security is maintained using commercially available equipment and industry-standard techniques, including performing periodic external vulnerability scanning and maintaining perimeter defenses, such as firewalls and intrusion prevention and detection.
- The infrastructure will at least be segmented into separate production systems and away from test and development environments.

- Antivirus and anti-malware programs are used on operating systems together with security configurations. The Provider's recommended security patches are deployed on both applications and operating systems in a timely manner.
- Updated malware protection is installed and maintained on all systems exposed to malware.
- Encryption is used on portable hard drives, other devices and portable media to the extent required to protect personal data. All personal data transmitted by the data processor is encrypted while in transit and at rest.
- Risk assessments are performed and documented using industry-recognized methodologies, such as the Cloud Security Alliance or equivalent, ISO 27001 or other independent schemes.
- Mobile device administration software is used to manage security controls on both corporate and employee devices used for business purposes.

Access management

- The Data Processor ensures that the Data Controller's personal data is only accessed by authorized persons using the procedures for access management, which ensure access on a "least privilege" basis, and that access is terminated where and when appropriate.
- The Data Processor has user administration procedures in place that define user roles and their privileges, and how access is granted, changed and terminated.
- The Data Processor performs regular checks of the assigned rights. The controls are documented and the documentation can be provided to the controller upon request.
- Systems used to process the Data Controller's personal data shall be further secured through multi-factor authentication and remote access to data. Programs and infrastructure shall have at least two-factor authentication.

Logging

- All login attempts are logged to register unauthorized access to personal data.
- All access to personal data is logged, and the access log includes the date and time of access, user ID and the type of access (read, edit, delete, search criteria, etc.).
- Security logging is activated on all network equipment, servers and on all applications, including databases and IT system administrators.

- A log of access to personal data and the use of personal data is monitored and regularly reviewed by the Data Processor in order to register unauthorized access to personal data.
- The Data Processor has a documented procedure for how often log files are reviewed and who has carried out the control. Documentation can be made available to the Data Controller upon request.

Backup

- The Data Processor performs a backup of the personal data processed on behalf of the Data Controller and has procedures in place to ensure the restoration of backed-up data in a timely manner to ensure accessibility and access to personal data.
- The Data Processor has a documented procedure for performing backup copying. Such a procedure has identified the requirements for storing and deleting data.
- The Data Processor has implemented procedures to verify backups upon successful re-introduction of backed up data, software and systems at least every six months.
- Backups are protected against unauthorized access, including destruction, and must be encrypted if the backup contains personal data where encryption based on a risk assessment is required.

Accessibility

- The Data Processor has implemented procedures for the effective detection, analysis and handling of security incidents to ensure the availability of personal data.
- The Data Processor has implemented a documented and tested disaster recovery plan and a business continuity strategy covering systems used to process personal data.
- Disaster recovery plans and business continuity strategies are tested and updated regularly and at least annually to ensure that they are up-to-date and effective. Documentation can be made available to the Data Controller upon request.