CREWVIE DATA PROCESSING AGREEMENT

This Data Processing Agreement ("**DPA**") forms part of the agreement between Customer (as defined below) and **Crewvie, Inc**. ("Company") for Company Offerings (as defined below) (collectively, the "Agreement"). For the purposes of this DPA, "Customer" means the entity or individual identified in the applicable Agreement for Company's product offerings and services (collectively, the "Company Offerings") and is a party to the Agreement and governs the parties' Personal Data Processing (both as defined herein) and related obligations. This DPA includes and incorporates by reference Appendices I, II, and III, including the Standard Contractual Clauses that govern the transborder transfer of Personal Data.

All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement. All references to the "Agreement" shall include this DPA (including the Standard Contractual Clauses and associated annexes listed in Appendix III of this DPA where applicable).

1. SUBJECT OF THE AGREEMENT

1.1. Pursuant to the Agreement, Company provides certain services to Customer ("Services").

1.2. In the course of providing the Services, pursuant to the Agreement, Company may process Protected Data (as defined herein) on behalf of Customer.

1.3. The parties agree to comply with the provisions of this DPA with respect to the Processing of any and all Protected Data provided to or collected by Company on behalf of Customer in relation to the provision or receipt of the Services by Customer, including Protected Data Processed under Data Protection Laws (as defined herein).

2. DEFINITIONS

2.1. "Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity.

2.2. "Appropriate Safeguard" means legally enforceable mechanism(s) for the transfer of Personal Data as may be permitted under Data Protection Laws at the time of such transfer.

2.3. "Customer User(s)" means the Data Subjects (as defined herein) set out in Annex I to the incorporated Standard Contractual Clauses (as defined herein).

2.4. "CCPA" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., all enacted and effective amendments thereto, and applicable implementing regulations.

2.5. "Data Controller" means the entity which determines the purposes and means of the Processing of Personal Data.

2.6. "Data Processor" means the entity which Processes Personal Data on behalf of the Data Controller, including, as applicable, any "service provider" or "contractor" as those terms are defined by the CCPA.

2.7. "Data Subject" means the identified or identifiable person to whom Personal Data relates.

2.8. "Data Subject Request" means a request made by a Data Subject to exercise any rights of said Data Subject under Data Protection Laws.

2.9. "Data Protection Laws" means any and all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland, the United Kingdom, and the United States and its states, applicable to the Processing of Personal Data under the Agreement as amended from time to time, including but not limited to EU Data Protection Laws and Non-EU Data Protection Laws.

2.10. "EU Data Protection Laws" means all data protection laws and regulations applicable to Europe, including (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (General Data Protection Regulation) ("GDPR"); (ii) Directive 2002/58/EC concerning the Processing of Personal Data and the protection of

privacy in the electronic communications sector; (iii) the Swiss Federal Act on Data Protection; (iv) applicable national implementations of (i) and (ii) of this subsection; and (v) in respect of the United Kingdom ("UK"), any applicable national legislation that replaces or converts in domestic law the GDPR or any other law relating to data and privacy as a consequence of the UK leaving the European Union).

2.11. "Europe" means, for the purposes of this DPA, the European Union, the European Economic Area ("EEA") and/or their member states, Switzerland and the UK.

2.12. "Non-EU Data Protection Laws" means the California Consumer Privacy Act ("CCPA"); the Canadian Personal Information Protection and Electronic Documents Act ("PIPEDA"); the Brazilian General Data Protection Law ("LGPD"), Federal Law no. 13,709/2018; and the Privacy Act 1988 (Cth) of Australia, as amended ("Australian Privacy Law").

2.13. "Personal Data" means any information relating to (i) an identified or identifiable natural person and (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws and Regulations).

2.14. "Personal Data Breach" means any actual breach of security leading to the accidental or unlawful access to or destruction, loss, alteration, or unauthorized disclosure of any Protected Data.

2.15. "Process" and "Processing" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic 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. Likewise, "Processor" means the entity that is Processing the Personal Data.

2.16. "Protected Data" means Personal Data relating to Customer Users and which is disclosed at any time to Company or Sub-Processors (as defined herein) by or on behalf of Customer in connection with this DPA and/or the Agreement.

2.17. “Sensitive Data” means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; genetic data, or biometric data for the purpose of uniquely identifying a natural person; data concerning health or a person’s sex life or sexual orientation; or data relating to criminal convictions and offenses.

2.18. “Standard Contractual Clauses” means Appendix III to this DPA pursuant to the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on Standard Contractual Clauses for the transfer of Personal Data to Processors established in non-European Union countries which do not ensure an adequate level of data protection. The Standard Contractual Clauses as listed in Appendix III to this DPA are heareby incorporated by reference into this DPA. The Standard Contractural Clauses may be updated from time to time in accordance with applicable Data Protection Laws. Such changes shall be incorporated into this DPA and the obligations of the parties without invalidating this DPA if such changes do not create an unreasonable financial, operational, or resources burden.

2.19. “Sub-Processor” means any Data Processor contracted with or directed by Company to Process Personal Data.

2.20. “Supervisory Authority” means any local, national or multinational agency, department, official, parliament, public or statutory person, or any government or professional body, regulatory or oversight authority, board, or other body responsible for administering Data Protection Laws.

2.21. As applicable to the CCPA or California residents, the definitions in this DPA of: “Data Controller” includes “Business”; "Data Processor" includes “Service Provider” and “Contractor”; “Data Subject” includes “Consumer”; and “Personal Data” includes “Personal Information”.

2.22. In this DPA references to any Data Protection Laws and to terms defined in such Data Protection Laws shall be replaced with or incorporate (as the case may be) references to

any Data Protection Laws replacing, amending, extending, re-enacting or consolidating such Data Protection Laws from time to time and the equivalent terms defined therein.

3. ROLES OF THE PARTIES

3.1. Unless otherwise specifically agreed in writing by the parties, the parties acknowledge and agree that with regard to the Processing of Personal Data pursuant to applicable Data Protection Laws, Customer is the Data Controller, Company is the Data Processor acting on behalf of Customer to Process Protected Data according to the nature and details of such Processing described in Appendix I, and that any subcontractors engaged by Company for the purpose of performing the Servies are Sub-Processors.

3.2. Company shall Process Protected Data only in accordance with Customer's documented lawful instructions as set forth in this DPA, as necessary to comply with applicable law, or as otherwise agreed in writing. The parties agree that the Agreement sets out Customer's complete and final instructions to Company in relation to the Processing of Protected Data, and Processing outside the scope of these instructions (if any) shall require prior written agreement between the parties. Company shall comply with the terms and conditions set forth in this DPA in its Processing of Protected Data and as required by Data Protection Laws.

3.3. Customer represents and warrants that it (i) has complied, and will continue to comply, with all applicable laws, including Data Protection Laws, in respect of its Processing of Protected Data and any Processing instructions it issues to Company; (ii) has provided, and will continue to provide, all required notices to Data Subjects; and (iii) has obtained, and will continue to obtain, all required consents and rights necessary under Data Protection Laws for Company to Process Protected Data for the purposes described in the Agreement. Customer shall have sole responsibility for the accuracy, quality, and legality of Protected Data and the means by which Customer acquired such Protected Data. Without prejudice to the generality of the foregoing, Customer agrees that it shall be responsible for complying with all laws (including Data Protection Laws) or other content created rights sent or managed through the Company Services, including those relating to obtaining consents and other valid legal bases where required to provide

Protected Data of any Data Subject to Company or upload Protected Data to the Company Services.

3.4. Customer will review Company's plan for Processing Protected Data and ensure such plan is in accordance with Customer's instructions will not cause Company to violate any applicable law, regulation, or rule, including, without limitation, Data Protection Laws.

4. PURPOSE LIMITATION

The Processing of Protected Data by Company for Customer is such as is required in the performance of the contracted Services under the Agreement.

5. OBLIGATIONS OF THE PROCESSOR FOR DATA PROTECTION

5.1. Company shall in relation to Protected Data Processed by Company on behalf of Customer as a Data Processor:

a) Process the Protected Data only on documented instructions from Customer. Customer's instructions may be specific instructions or standing instructions of general application in relation to the performance of Company's obligations under the Agreement;

b) warrant that anyone authorized by Company to Process Protected Data ("Authorized Persons") shall be subject to a duty of confidentiality by contract and/or by law, where applicable. Company shall ensure that all Authorized Persons have signed an appropriate confidentiality agreement, are otherwise bound to a duty of confidentiality, or are under an appropriate statutory obligation of confidentiality. Company shall not permit any person not subject to confidentiality to Process Protected Data. Company will ensure that only Authorized Persons will have access to and will Process Protected Data. Company will ensure that such access and Processing of Protected Data is limited to the extent necessary for the provision of the contracted Services;

c) take reasonable measures required pursuant to Article 32 of GDPR with respect to the security of Processing;

d) adhere to the requirements of Data Protection Laws for engaging a Sub-Processor;

e) taking into account the nature of the Processing, assist Customer by technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to any complaint relating to the Processing of Protected Data by Company. Company will cooperate with Customer with respect to any action taken relating to such request or complaint;

f) reasonably assist Customer in complying with Customer's obligations under Data Protection Laws with respect to:

i) security of Processing;

ii) notifications to a Supervisory Authority in case of any Personal Data Breach;

iii) communications to Data Subjects by Customer in response to any Personal Data Breach;

iv) data protection impact assessments (as such term is defined in Data Protection Laws);

v) prior consultation with a Supervisory Authority regarding high-risk Processing;

g) at Customer's choice, delete or return all the Protected Data to Customer, and require that all third parties supporting Company's Processing of the Protected Data take the same action:

i) once Processing by Company of any Protected Data is no longer required for the purpose of Company's performance of its relevant obligations under the Agreement;

ii) upon termination of the Agreement; or

iii) on request by Customer; and

iv) delete existing copies of such Protected Data, unless Data Protection Laws require storage of the Protected Data, in which case, Company shall inform Customer of any such requirements; and

v) make available to Customer all information necessary to demonstrate compliance with the obligations of this DPA and allow for and assist in reasonable audits conducted by Customer.

5.2. Company shall promptly notify Customer, unless prohibited from doing so under Data Protection Laws, if it becomes aware or believes that any Protected Data Processing instruction from Customer violates Data Protection Laws or if Company is unable to comply with such instruction for any other reason.

5.3. Company may de-identify or aggregate Personal Data as part of performing the Service specified in this DPA and the Agreement.

6. DATA SUBJECT RIGHTS REQUESTS

6.1. Upon receipt of a Data Subject Request, Customer shall attempt to resolve the Data Subject Request in the first instance. Company shall reasonably co-operate, as requested by Customer, to enable Customer to comply with the exercise of rights by a Data Subject under any Data Protection Laws in respect of Protected Data and comply with any assessment, inquiry, notice or investigation under any Data Protection Laws in respect of Protected Data or the Agreement, or this DPA.

6.2. Company shall notify Customer if it receives a complaint, communication, or request from a Data Subject under any Data Protection Laws and shall provide full details of that request.

6.3. Company shall not respond to any Data Subject, Customer User, or Consumer rights request relating to Personal Data unless required by Data Proection Laws or other laws or in Company's sole discretion, if expressly instructed to do so by Customer.

6.4. To execute on a deletion request, Company shall securely delete the relevant Protected Data in question and shall confirm such deletion to Customer. Company shall inform Customer, if Company is unable to delete Protected Data or otherwise unable or unwilling to respond to, or assist with, a Data Subject Request. In such case, Company shall provide Customer with the records of relevant Protected Data then in Company's possession or control, in a readable form for Data Subject's internal use.

6.5. Company's obligations regarding Data Subject Requests, shall apply to Consumer's rights under the CCPA.

7. CONFIDENTIALITY

Company shall ensure that Authorized Persons engaged in the Processing of Protected Data are informed of the confidential nature of the Protected Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements. Company shall ensure that such confidentiality obligations survive the termination of the personnel engagement per the requirements of applicable Data Protection Laws.

8. RECORDS, INFORMATION AND AUDIT

Company shall maintain, in accordance with Data Protection Laws binding on Company, written records of all categories of Processing activities carried out on behalf of Customer.

9. SUB-PROCESSORS

9.1. Customer acknowledges that the provision of the Services by Company requires the use of Sub-Processors. Customer agrees that Company may engage Sub-Processors to

Process Protected Data on Customer's behalf. Company shall utilize Sub-Processors in accordance with this section and Appendix I to this DPA..

9.2. Company shall enter into a written agreement with each Sub-Processor containing data protection obligations that provide at least the same level of protection for Protected Data as those in this DPA, to the extent applicable to the nature of the service provided by such Sub-Processor. Where a Sub-Processor fails to fulfill its data protection obligations, Company shall remain liable to Customer for the performance of the Sub-Processor's obligations, subject to the terms of the Agreement, including this DPA.

9.3. Customer grants to Company general authorization for sub-Processing by third parties in order to support the performance of the Services including data center operators, email service providers, providers of fraud detection/authenticity services, outsourced support providers, and others. Company shall keep Customer informed of all Sub-Processors engaged in the provision of the Services. Customer may object to additions of or changes in Sub-Processor on reasonable grounds based on non-compliance or a material risk of non-compliance by Sub-Processor with Data Protection Laws or this DPA.

9.4. When Sub-Processors Process Personal Data, Company shall take steps to ensure that such Sub-Processors are Service Providers under the CCPA with whom Company has entered into a written contract that includes terms substantially similar to this DPA or are otherwise exempt from the CCPA's definition of "sale." Company shall conduct appropriate due diligence on its Sub-Processors.

10. SECURITY

10.1. Company shall implement and maintain appropriate technical and organizational security measures that are designed to protect Protected Data from Personal Data Breaches and designed to preserve the security and confidentiality of Protected Data. In relation to the Processing of Protected Data, Company shall implement and maintain, at its cost and expense, an information security program taking into account the state of art, the costs of implementation and the nature, scope, context and purposes of Processing the Protected Data. Such program shall include technical and organizational measures no less stringent

than those set out in Appendix II of this DPA and, where applicable, Annex II to the included Standard Contractual Clauses contained in Appendix III.

10.2. Notwithstanding the above, Customer agrees that except as provided by this DPA, Customer is responsible for its secure use of the Service, including securing its account authentication credentials, protecting the security of Protected Data when in transit to and from the Service, and taking any appropriate steps to securely encrypt or backup any Protected Data uploaded to the Service.

11. AUDIT

On an annual basis, Company shall (i) audit its physical, technical, and administrative safeguards in place to protect Protected Data; (ii) make available to Customer, on request, all information necessary to demonstrate compliance with this DPA; (iii) permit Customer or another auditor mandated by Customer to inspect, audit and copy any relevant records, processes and systems in order that Customer may satisfy itself that the provisions of Data Protection Laws and this DPA are being complied with; (iv) provide reasonable cooperation to Customer in respect of any such audit; and (v) at the request of Customer, provide Customer with evidence of compliance with its obligations under this DPA. Customer shall bear all costs associated with such audits.

12. INTERNATIONAL DATA TRANSFERS

12.1. Subject to applicable Data Protection Laws, Customer acknowledges that Company may transfer and Process Protected Data to and in the United States and anywhere else in the world where Company, its Affiliates or its Sub-Processors maintain data Processing operations. Company shall at all times ensure that such transfers are made in compliance with the requirements of Data Protection Laws and this DPA. The provisions of this DPA shall constitute Customer's instructions with respect to transfers.

12.2. To the extent that Company is a recipient of Protected Data protected by the Australian Privacy Law, the parties acknowledge and agree that Company may transfer such Protected Data outside of Australia as permitted by the terms agreed upon by the parties and subject to Company complying with this DPA and the Australian Privacy Law.

12.3. To the extent Company is a recipient of Protected Data protected by EU Data Protection Laws ("EU Data") in a country outside of Europe that is not recognized as providing an adequate level of protection for Personal Data (as described in applicable EU Data Protection Law), the parties agree to the following:

12.3.1. Company agrees to abide by and Process EU Data in compliance with the Standard Contractual Clauses in the form set out in Appendix III hereto. For the purposes of the descriptions in the Standard Contractual Clauses, the parties agree that Company is the "Data Importer" and Customer is the "Data Exporter," even in cases where Customer may itself be an entity located outside Europe.

12.4. To the extent Company adopts an alternative data export mechanism not described in this DPA (including any new version of or successor to the Standard Contractual Clauses or Privacy Shield) ("Alternative Transfer Mechanism") for the transfer of EU Data, the Alternative Transfer Mechanism shall apply instead of the transfer mechanisms described in this DPA (but only to the extent such Alternative Transfer Mechanism complies with applicable EU Data Protection Law and extends to the countries to which EU Data is transferred). In addition, if and to the extent that a court of competent jurisdiction or Supervisory Authority orders (for any reason) that the measures described in this DPA cannot be relied on to lawfully transfer EU Data (within the meaning of applicable EU Data Protection Law), Company may implement any additional measures or safeguards that may be reasonably required to enable the lawful transfer of EU Data.

13. OBLIGATIONS OF THE CUSTOMER

13.1. Customer warrants and represents that all Protected Data relating to Customer Users disclosed or made available to Company will have been collected or made available in accordance with Data Protection Laws, including in respect of any required notifications, information, transparency or consents and that the collection, Processing, and use of such Protected Data by Company on behalf of Customer in accordance with this DPA will not result in any contravention of Data Protection Laws.

13.2. Customer represents and warrants that: (i) all instructions given by it to Company in respect of Protected Data shall at all times be in accordance with Data Protection Laws and (ii) Customer shall not unreasonably withhold, delay or condition its agreement to any change to this DPA requested by Company in order to ensure the Services comply with Data Protection Laws.

13.3. Customer represents and warrants that it has all necessary rights to provide the Personal Data to Company for the Processing to be performed in relation to the Agreement. To the extent required by applicable Data Protection Law, Customer is responsible for ensuring that any necessary Data Subject consents to this Processing are obtained, and for ensuring that a record of such consents is maintained. Should such consent be revoked by the Data Subject, Customer is responsible for communicating the fact of such revocation to Company, and Customer remains responsible for implementing any Customer instruction with respect to the further Processing of such Personal Data.

14. REPORTING PERSONAL DATA BREACHES

Upon becoming aware of a Personal Data Breach, Company shall: (i) notify Customer without undue delay, and where feasible, no later than 48 hours after becoming aware of a Personal Data Breach affecting Customer Protected Data; (ii) provide timely information relating to the Personal Data Breach as it becomes known or as is reasonably requested by Customer; (iii) complete a commercially reasonable forensic investigation of the Personal Data Breach, consistent with industry standards, and share with Customer the results of such investigation; (iv) promptly take reasonable steps to contain and investigate any Personal Data Breach; and (v) cooperate with Customer as reasonably necessary to facilitate compliance with Data Protection Laws and any other applicable laws and regulations. Company's notification of or response to a Personal Data Breach shall not be construed as an acknowledgment by Company of any fault or liability with respect to such Personal Data Breach.

15. LIMITATION OF LIABILITY

Each party’s and all of its Affiliates’ liability taken together in the aggregate arising out of or related to this DPA (including the Standard Contractual Clauses) shall be subject to the exclusions and limitations of liability set forth in the Agreement. Any claims made against Company or its Affiliates under or in connection with this DPA (including, where applicable, the Standard Contractual Clauses) shall be brought solely by the Customer entity that is a party to the Agreement. This section notewithstanding, in

no event shall any party limit its liability with respect to any Data Subject's data protection rights under this DPA or otherwise.

16. GENERAL PROVISIONS

16.1. Regarding the subject matter stated herein, this DPA, including the annexes attached hereto, constitutes the entire agreement between the parties, and supersedes all previous communications, representations, understandings, and agreements, either oral, electronic, or written. Except for any changes made by this DPA, the Agreement remains unchanged and in full force and effect.

16.2. The parties agree that this DPA shall replace any existing DPA, similar Personal Data Processing agreement or document, and conflicting clause related to Personal Data Processing in the Agreement that the parties may have previously entered into in connection with the Service. Changes and amendments to this DPA and any of its components require written agreement between Company and Customer.

16.3. This DPA shall remain in effect for as long as Company carries out Protected Data Processing operations on behalf of Customer or until termination of the Agreement, whichever is later. It is the intention of the parties that no one other than a party to this DPA, its successors, and permitted assignees shall have any right to enforce any of the terms of this DPA.

16.4. In the event of any conflict or inconsistency between this DPA and the Agreement, the Standard Contractual Clauses, the Company Standard Terms of Service, or the Company website Privacy Policy, the provisions of the following documents (in order of precedence) shall prevail: (i) Standard Contractual Clauses; then (ii) this DPA; then (iii) the Agreement; then (iv) the Company Terms of Service; and then (v) the Company website Privacy Policy.

16.5. This DPA shall be governed by and construed in accordance with the governing law and jurisdiction provisions in the Agreement, unless required otherwise by applicable Data Protection Laws.

Appendix I

Subject Matter and Details of the Data Processing

This Appendix 1 is incorporated into this DPA, and also forms part of the Standard Contractual Clauses (if such Standard Contractual Clauses are applicable to Customer).

Data Processor / Data Importer

The Data Importer (or Service Provider/Contractor/Processor) is Company.

Data Controller / Data Exporter

The Data Exporter (or Business/Controller) is the Customer that is a party to this DPA.

Subject Matter

Company's provision of the Services to Customer and Processing of Protected Data as set forth in the Agreement, including and this DPA.

Duration of the Processing

During the term of the Agreement and provision of the Company Services to Customer, and afterwards for so long as is necessary to fulfill the purposes for which it was collected, and as otherwise agreed upon in writing between the parties, and until deletion of all Customer Protected Data by Company in accordance with this DPA, or as required by applicable law, or.

Nature and Purpose of the Processing

Processing of identified Data Subjects' categories of Personal Data in order to provide, manage, and assess use of Company's Services, to provide the Company Offerings pursuant to the Agreement and the Company Terms of Service (https://crewvie.com/terms), and as instructed by Customer in its use of the same.

Categories of Data

- Device and Activity information
    - Server Logs (Contain IP Addresses)
    - Computer/Device Information

    - Browser Type
    - Software and Hardware Information
    - Geolocation Data
- Account
    - Full Name
    - Email Address
    - Password
    - Current Location
    - Job Title
    - Job Department
- Optional Demographic Information
    - Current Employer
    - Employment History
    - Contact Phone Number
    - Language Spoken
    - Production City
    - Industry Association
    - Union/Guild Affiliation
    - Experience Level
    - Work Experience
    - Education Experience
    - Industry Awards
    - Travel Preference
    - Industry Preference
    - Budget Preference
    - Availability
    - Team Contacts, Including Information About Your Assistant, Attorney, Agent And Manager
    - Links To Your Social Media Profiles (Including IMDB, Website, LinkedIn, Instagram, Facebook, And Twitter)
    - Race And Ethnicity
    - Gender Identity
    - Disability Self-Identification
    - Military Experience

    - Age
    - Census Information
- Mailing Lists and Support Requests
    - Contact Information
    - Email Address
    - Messages, including any optional confidential and/or Sensitive Data contained within the message
    - Postal Mailing Address, if provided
- Surveys and Forms
    - Contact Information
    - Association with Account and/or other Demographic Information
- Public Posts
    - Profile Information, including, but not limited to, Name, Contact Information, Thumbnail
    - Posted Content
- Social Media
    - Login Access
    - Social Media ID of User Name
    - Additional Information Based on the Sharing Settings of the Social Media Platform, which may include email address, friend lists, posts on the Social Media Platform
- Analytics
    - Website Browsing Information
    - Product Usage Information
    - Transaction Information
- Other Collections
    - Publicly Available Information
    - Commercially Available Information
    - Shared Information from Affiliates and Business Customers
    - Data Subjects
        - End users of Company Offerings;
        - Employees, contractors, agents, vendors, and advisors of Customer/Data Exporter.
        - Sub-Processors

- Customer hereby consents to Company's use of Sub-Processors. Company shall provide a list of Sub-Processors along with the nature, purpose, and locations of Personal Data being processed in Appendix IV.

Appendix II

Security

Company will implement and maintain industry standard technical and organizational security as set forth herein. Company may update or modify such security measures from time to time, provided that such updates and modifications do not materially decrease the overall security of the Services.

1. PREVENTION OF UNAUTHORIZED ACCESS TO PREMISES AND INSTALLATIONS USED FOR PROCESSING PERSONAL DATA.

a. Physical access to corporate sites is controlled via badge access, which is to be present with the employee at all times. All employees and contractors requiring physical access to the site receive this access during the new hire onboarding procedure controlled by the human resources department, and upon separation from Company, a termination procedure also owned by the human resources department, the badge/key authority is revoked.

b. Suppliers, Service Providers, Contractors, and other visitors requiring temporary access to the site are identified and monitored. All contract workers are required to sign in at the security desk where a badge is issued allowing access to only required areas. Visitors register at the security desk, are issued a temporary visitor identification tag, and are to be escorted at all times.

c. Specifically regarding critical IT areas (wiring closets, data center and co-location facilities), physical access is restricted to those with a legitimate business need (IT operations, network engineers, system administrators, etc.), managed by the IT department with approvals by VP (or a person holding an equivalent position) of IT. The doors to the co-location facility are locked at all times, accessible only via programmed badges. Visitor and contractors needing temporary access to the critical IT areas are required to sign in on the visitor log on entry and must be escorted by an employee with proper authority and access at all times. On a quarterly basis, IT management reviews the badge access list for unauthorized or terminated employees. In addition, on a quarterly

basis, a generic badge is tested against the critical IT area and the results are captured in the monthly reject report.

d. Only employees of the contractors have access to the server/operational data level as physical operation duties are the responsibility of the hosting providers. This access is verified using a biometric fingerprint scanner, proximity access cards (PAC) or similar measures.

e. Access controls restrict access by unauthorized employees to critical technical areas if they are not accompanied by a suitably authorized person.

f. All access is logged and strictly monitored.

g. A regular audit is performed of all data center access inspection logs (visitors, suppliers and guests), which is reviewed each month and initialed by the data center manager.

h. Surveillance cameras with cameras/digital video recorders (DVRs) or similar security measures are used around the clock in the inspection zones in all the internal and external installations.

2. PREVENTION OF UNAUTHORIZED ACCESS TO IT SYSTEMS

a. No shared logins or accounts.

b. Passwords are to be at least 8 characters long and comply with at least three of the four complexity requirements. They must be changed every 90 days and the last ten passwords cannot be used.

c. Access to data centers requires two-factor authentication. All logins, logoffs, and errors are logged.

d. Access to IT systems (network equipment, devices, servers, and applications) is controlled by end user access management or a similar policy. Separation of duties exists for all systems where access is requested, approved, and granted by different individuals

with proper business permissions to do so. Procedures are in place to grant rights to systems per business need, validate that business need on a quarterly basis, update authorities based on role changes within Company, and revoke access upon termination. All systems are accessed via a unique id with strong authentication and specific password syntax rules.

e. Remote access to Company's corporate infrastructure is controlled via VPN, using two-factor authentication. Access to VPN is granted only for Company employees, controlled via Active Directory, and managed by operations new hire/termination procedures.

f. Company's wireless network is secured according to industry standards and leverages a minimum of a 128-bit key. Two wireless networks are provided, one for guest access with a published password on the intranet, and one for employees with access to a corporate network where access is pre-configured by IT personnel on authorized equipment.

3. DATA ACCESS CONTROLS

a. Authorized Persons only have access to Personal Data which is in their area of responsibility and, where Processing Personal Data, that this data cannot be read, copied, changed or deleted without appropriate authorization.

b. Employees working in the operational area only are authorized to access the database and administer it, and also to modify and delete data. The logins and all database accesses of all employees working in the operational area are logged.

c. The Authorized Person assigned to Customer has access to Customer data and can view and Process these, but only using tools from Company and not via the interface of the database management system. All changes to the data made using these tools are logged.

d. Sensitive Data stored on any media is encrypted.

e. Sensitive Data transmitted over public or wireless networks is encrypted.

4. DISCLOSURE CONTROL

a. The data in Company's databases are protected during transfer between Customer and Company using SSL encryption.

b. The token assigned uniquely to a Customer User or Data Subject and used to identify said Data Subject is encoded before transfer to Company using a unique, Customer-specific SHA-256 token (or MD5 hash where SHA-256 is not supported by Customer) which is supplied to Customer as a key.

5. INPUT CONTROL

a. The administration tasks performed on servers are logged by the IT department, including the bash and login history.

b. All data manipulations including addition, deletion, approval or rejection of content data are logged using Company's content moderation system.

c. Logging of all data changes is also performed via Company's content moderation system.

6. JOB CONTROL

a. Background checks are performed on all new employees.

b. These background checks are also required for all Sub-Processors and other vendors of Company and must be performed by such Sub-Processors and vendors.

c. There are training courses for new employees of the operations and IT department. New employees have only limited access rights until the training measures have been completed during the first week of employment.

d. All work is inspected in accordance with the peer review principle, ensuring that all system changes are reviewed in advance by two people.

e. A violation of Company's protocols and procedures, if serious, results in immediate sanctions up to and including the withdrawal of all access rights and, where appropriate, termination.

7. AVAILABILITY CONTROL

a. Company maintains a business continuity plan which applies to procedures critical to Company's operations and aims to ensure that Personal Data is protected from accidental destruction or loss.

b. Company also uses failover backup systems so that operation is not interrupted if a catastrophic event occurs in the primary data center. Production databases are replicated in real time across geographically dispersed sites. Backup copies of the data are made daily.

c. 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.

d. Virus protection is required on all desktop and laptop computers in Company's network. Intrusion detection systems (IDSs) are used on all corporate networks to warn of any attacks.

e. Restorations of backup copies are tested regularly.

f. All source code, build, and configuration elements are managed in a source code repository that is backed up to two geographically dispersed sites daily.

8) SECURITY TESTING AND EVALUATION

a. Internal and external vulnerability scans are performed quarterly by Company's security team. The results are documented, reviewed by the information security officer (ISO) and prioritized by the cross-organizational security leadership team. Critical and high findings

are closed within 30 days pending environmental impact, and informational findings are acted upon on a case by case basis in line with risk management procedures. Network service is disabled for any vulnerability that cannot be closed in the allowable timeframe dependent upon risk.

b. An external penetration test is performed annually by a third party. The results are documented, reviewed by the ISO and delivered to Customer for review. Findings are documented and resolved following the change management procedures within timelines per severity.

c. Security event logs from anti-virus software, IDS/IPS, VPN, firewalls, spam filters and directory servers are captured via log management software and analyzed by a SOC. Critical events trigger automated alerts. Suspicious log events are reviewed by the IT team and acted upon in accordance with incident management procedures.

d. System and application events and audit records such as failed events, significant successful events, large file size download, frequency of transactions, application failures, configuration changes, authentication attempts, file accesses, account changes, and use of privileges are captured via log management software and analyzed by IT and development personnel where necessary. Critical events trigger automated alerts. Suspicious log events are reviewed by the IT Leadership and ISO and acted upon in accordance with incident management procedures.

e. Logs are retained for a period of 30 days for all system event logs, 1 year for security event logs and 1 year for any log capturing security incident information. Logs are stored on separate log infrastructure.

9. SEPARATION CONTROL

a. Customer data in data centers is logically separated and stored using a unique customer ID.

b. Customer data of others of Company's clients cannot be accessed under any circumstances.

c. For audits and quality assurance, Company uses a copy of Customer data.

d. Due to the nature of their role, employees of the operations department have unlimited access to Customer data.

e. Implementation engineers only have access to the data related to projects for which they are responsible, and only via tools supplied by Company.

Appendix III

STANDARD CONTRACTUAL CLAUSES

Controller to Processor

SECTION I

Clause 1. Purpose and scope

a. The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ( ) for the transfer of data to a third country.

b. The Parties:
   i. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and
   ii. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer') have agreed to these standard contractual clauses (hereinafter: 'Clauses').

c. These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

d. The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2. Effect and invariability of the Clauses

a. These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to

processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

b. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3. Third-party beneficiaries

a. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:'
   i. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
   ii. Clause 8.1b, 8.9a, c, d and e;
   iii. Clause 9a, c, d and e;
   iv. Clause 12a, d and f;
   v. Clause 13;
   vi. Clause 15.1c, d and e;
   vii. Clause 16e;
   viii. Clause 18a and b.

b. Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4. Interpretation

a. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

b. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

c. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5. Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6. Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7. Optional Docking Clause

a. An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

b. Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

c. The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8. Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

1. Instructions

    a. The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of

the contract.

b. The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

2. Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

3. Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

4. Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

5. Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as

long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

6. Security of processing

    a. The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

    b. The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

    c. In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more

information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

d. The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

7. Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8. Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ( ) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

i. the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

ii. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

iii. the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

iv. the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

9. Documentation and compliance

   a. The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

   b. The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

   c. The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

   d. The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

   e. The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9. Use of sub-processors

a. SPECIFIC PRIOR AUTHORISATION

The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least [Specify time period] prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

b. Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. ( ) The Parties agree that, by complying with this Clause, the data importer fulfills its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

c. The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

d. The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfill its obligations under that contract.

e. The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10. Data subject rights

a. The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

b. The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

c. In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11. Redress

a. The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

b. In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

c. Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

    i. lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
    ii. refer the dispute to the competent courts within the meaning of Clause 18.

d. The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

e. The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

f. The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12. Liability

a. Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

b. The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

c. Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

d. The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

e. Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

f. The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

g. The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13. Supervision

a. [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

b. The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14. Local laws and practices affecting compliance with the Clauses

1. The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

2. The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

    a. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

    b. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

    c. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

3. The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

4. The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

5. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

6. Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfill its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15. Obligations of the data importer in case of access by public authorities

7. Notification

    a. The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

i. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

ii. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

b. If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

c. Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

d. The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

e. Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

8. Review of legality and data minimisation

a. The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

b. The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

c. The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16. Non-compliance with the Clauses and termination

a. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

b. In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

c. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

   i. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

   ii. the data importer is in substantial or persistent breach of these Clauses; or

   iii. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

   In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

d. Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

e. Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17. Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of the Netherlands.

Clause 18. Choice of forum and jurisdiction

a. Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

b. The Parties agree that those shall be the courts of the Netherlands.

c. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

d. The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as Data Exporter(s) and/or Data Importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

Data Exporter(s)

Name: Customer

Address: : As stated in Customer's underlying Agreement

Contact person's name, position and contact details: The Contact information provided by Customer in its Account

Activities relevant to the data transferred under these Clauses: To provide the Company Offerings pursuant to the Agreement, as defined in the encompassing Data Processing Agreement.

Signature and date: The signature and date provided by the party identified as Customer within the encompassing Data Processing Agreement in execution of said Data Processing Agreement, which incorporates Customer's agreement to these Standard Contractual Clauses by reference to Appendix III of said Data Processing Agreement.

Role (controller/processor): Controller

Data Importer(s):

Name: Crewvie, Inc.

Address: Attn: Business and Legal Affairs 111 W. Grand Avenue El Segundo, CA. 90245

Contact person's name, position and contact details: As described in Customer's Underlying Agreement

Activities relevant to the data transferred under these Clauses: To provide the Company Offerings pursuant to the Agreement, as defined in the encompassing Data Processing Agreement.

Signature and date: The signature and date provided by Company in execution of the encompassing Data Processing Agreement, which incorporates Company's agreement to these Standard Contractual Clauses by reference to Appendix III of the Data Processing Agreement

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

- End users of Company products and services;
- Employees, contractors, agents, vendors, and advisors of Data Exporter.
- Customer Users of Data Exporter

Categories of Personal Data transferred
See Appendix I of this DPA.

Sensitive Data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as, for instance, strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to such Sensitive Data, restrictions for onward transfers, and/or additional security measures.

Company does not require Sensitive Data to be shared with Company or transferred. Company does, however, share and may transfer Sensitive Data if a Data Subject elects to share it with Company in accordance with the Company Privacy Policy found on https://crewvie.com/privacy.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).
See Appendix I of this DPA.

Nature of the processing

See Appendix I of this DPA.

Purpose(s) of the data transfer and further processing

See Appendix I of this DPA.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

See Appendix I of this DPA.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Company engages third party Sub-Processors to provide or assist in providing portions of the Company Services and works to ensure any such Sub-Processors adhere to applicable Data Protection Laws and privacy laws and Process any Personal Data only to provide their contracted for products or services in accordance with Company's instructions and not for any other purpose. The list of Company's Sub-Processors' is provided in Appendix IV.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

California Attorney General

California Privacy Protection Agency

The Supervisory Authority of the country of residence of the Data Subject

ANNEX II

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

EXPLANATORY NOTE:

The technical and organizational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organizational measures implemented by the Data Importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Company provides numerous technical and organizational measures to ensure the security of the data it processes as identified in Appendix II to this DPA.

For transfers to (Sub-) Processors, also describe the specific technical and organizational measures to be taken by the (Sub-) Processor to be able to provide assistance to the Controller and, for transfers from a Processor to a Sub-Processor, to the Data Exporter

Company works to ensure any Sub-Processors adhere to applicable Data Protection Laws and process any Personal Data only to provide their contracted for products or services, in accordance with Company's instructions and not for any other purpose. Further, Company shall require that its Sub-Processors provide at least the technical and organizational measures identified in Appendix II of this DPA.

ANNEX III

LIST OF SUB-PROCESSORS

EXPLANATORY NOTE:

This Annex must be completed in case of the specific authorization of Sub-Processors (Clause 9(a), Option 1).

The Controller has authorized the use of the Sub-Processors. Company shall provide a list of Sub-Processors in Appendix IV of this DPA.

Appendix IV

COMPANY'S SUB-PROCESSORS

Sub-Processor/Legal Entity	Nature of Processing	Location
Microsoft Corporation (Azure)	Hosting	United States
Amazon Web Services, Inc.	Hosting (other than in Europe, the Middle East, and Africa)	United States