COMMAND ALKON INCORPORATED DATA PROCESSING ADDENDUM

Updated: 07/21/22

This Data Processing Addendum ("**DPA**") forms part of the *Master License and Services Agreement* ("**Agreement**") between: (i) Customer (identified in the signature line below) and its EEA affiliates **("Customer")**; and (ii) Command Alkon Incorporated and its affiliates ("**Company**").

In consideration of the applicable General Data Protection Regulation ("GDPR"), this Addendum supersedes any previous agreement between the parties regarding the subject matter herein, i.e., data privacy and security as applicable to the GDPR.

In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Agreement.

1. Definitions

"**Customer Personal Data**" means personal data Processed by Company on behalf of Customer in provision of the Products and/or Services.

"**Data Subject**" means the individual to whom Customer Personal Data relates.

"**Data Protection Laws**" means the General Data Protection Regulation (EU) 2016/679 on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC (and any amendment or replacement to it), the Swiss Federal Data Protection Act of 19 June 1992 (and any amendment or replacement to it), or the EU GDPR as amended and incorporated into UK law under the UK European Union (Withdrawal) Act 2018 and applicable secondary legislation made under that Act (and any amendment or replacement to it), depending on which is applicable

"**Personal Data**" means any information that relates to a Data Subject, including but not limited to a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the Data Subject.

"**Privacy Shield**" means the EU-U.S. Privacy Shield legal framework and the Swiss-U.S. Privacy Shield legal framework. While both frameworks are currently inoperable, Company continues to adhere to their requirements, and this term will apply to any renewed and approved version of the Privacy Shield agreement between the United States and the European Economic Area ("EEA").

"**Process**" or "**Processing**" means any operation or set of operations which is performed on Customer Personal Data, whether or not by automated means, such as the collection, recording, organization, structuring, storage, alteration, retrieval, consultation, use, disclosure, disposal, restriction, access, dissemination, combination, adaption, copying, transfer, erasure and/or destruction of Customer Personal Data.

“**Security Breach**” means a breach of security leading to an accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Personal Data transmitted, stored, or otherwise processed.

“Third Party” means a party other than Customer or Company.

The terms “**controller**”, “**processor**”, and “**supervisory authority**” as used in this DPA will have the meanings ascribed to them in the GDPR.

All other non-defined but capitalized terms shall have the meaning set forth in the Agreement.

2. Processing of Customer Personal Data

2.1 Purpose of Processing. The purpose of data Processing under this DPA is the provision of the Products and/or Services pursuant to the Agreement. Annex 1 describes the subject matter and details of the Processing of Customer Personal Data.

2.2 Processor and Controller Responsibilities. The parties acknowledge and agree that: (a) Company is a processor of Customer Personal Data under the Data Protection Laws; (b) Customer is a controller of Customer Personal Data under the Data Protection Laws; and (c) each party will comply with the obligations applicable to it under the Data Protection Laws with respect to the Processing of Customer Personal Data.

2.3 Customer Instructions. Customer instructs Company to Process Customer Personal Data: (a) in accordance with the Agreement and any applicable Supplement; (b) as otherwise necessary to provide the products and/or services to the Customer; (c) as necessary to comply with applicable law or regulation; and (d) to comply with other reasonable written instructions provided by Customer where such instructions are consistent with the terms of the Agreement. Customer will ensure that its instructions for the Processing of Customer Personal Data shall comply with the Data Protection Laws. As between the parties, Customer shall have sole responsibility for the accuracy, quality, and legality of Customer Personal Data and the means by which Customer obtained the Customer Personal Data.

2.4 Company’s Compliance With Customer Instructions. Company shall only Process Customer Personal Data in accordance with Customer’s instructions and shall treat Customer Personal Data as confidential information. If Company believes or becomes aware that any of Customer’s instructions conflict with any Data Protection Laws, Company shall inform Customer within a reasonable timeframe. Company may Process Customer Personal Data other than on the written instructions of Customer if it is required under applicable law to which Company is subject. In this situation, Company shall inform Customer of such requirement before Company Processes the Customer Personal Data unless prohibited by applicable law.

3. Sub-processors

3.1 Appointment of Sub-processors. Customer hereby provides general written authorization for Company to engage third-party sub-processors to provide limited or ancillary services in connection with the provision of products and/or services. The Company website lists sub-processors that are currently engaged by Company to carry out specific processing activities related to Customer Personal Data and Company will update the sub-processor list prior to engaging any new sub-processor to carry out specific processing. Customer may sign up for electronic updates any time the Company sub-processor list is changed. Customer may object to any sub-processor by communicating such objection to Company within thirty (30) days of an update, and the parties will work in good faith to resolve the objection. Customer hereby agrees to sub-processing activities by current sub-processors listed on the Company's website.

3.2 Sub-processor Security. Where Company subcontracts its obligations, it shall do so only by way of a written agreement with the sub-processor which imposes contractual obligations that are at least equivalent to those obligations imposed on Company under this Addendum.

3.3 Liability. Where the sub-processor fails to fulfill its data protection obligations under such written agreement, Company shall remain fully liable to Customer for the performance of the sub-processor's obligations under such agreement.

4. Security and Privacy Impact Assessments

4.1 Company Security. Company will implement appropriate technical and organizational measures to safeguard Customer Personal Data ("Information Security Program") taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of Processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. Company's current technical and organizational measures are listed in Annex II to the Standard Contractual Clauses (attached) and Company governs itself under the following security standards: NIST 800-171; AWS CIS.

4.2 Customer Security. Customer acknowledges the products and/or services include certain features and functionalities that Customer may elect to use which impact the security of Customer Personal Data processed by Customer's use of the products and/or services. Customer is responsible for reviewing the information Company makes available regarding its data security and making an independent determination as to whether the products and/or services meet the Customer's requirements and legal obligations, including its obligations under applicable Data Protection Law. Customer is further responsible for properly configuring the products and/or services and using features and functionalities made available by Company to maintain appropriate security in light of the nature of Customer Personal Data processed as a result of Customer's use of the products and/or services for. Customer is responsible for its use of the products and/or services and its storage of any copies of Customer Personal Data outside Company's or Company's sub-processors' systems including, but not limited to, securing the account authentication credentials, systems and devices, and retaining copies of its Customer Personal Data as appropriate.

4.3 Company Personnel. Company shall ensure that its personnel engaged in the Processing of Customer Personal Data are informed of the confidential nature of the

Customer Personal Data and are subject to obligations of confidentiality, with such obligations surviving the termination of that individual's engagement with Company.

4.4 Security Testing. Company will test, assess, and evaluate the effectiveness of the Information Security Program for ensuring the secure Processing of Customer Personal Data. Company will comply with its Information Security Program and represents and warrants that its Information Security Program is and will be in compliance with applicable law.

4.5 Impact Assessments. Company will take reasonable measures to cooperate and assist Customer in conducting impact assessments and related consultations with any supervisory authority, if Customer is required to conduct such impact assessments under Data Protection Laws.

5. Data Subject Rights

5.1 Assistance with Customer's Obligations. To the extent Customer, in its use or receipt of the products and/or services, does not have the ability to correct, amend, restrict, block or delete Customer Personal Data as required by Data Protection Laws, Company shall promptly comply with reasonable requests by Customer to facilitate such actions to the extent Company is legally permitted and able to do so. If legally permitted, Customer shall be responsible for any cost arising from Company's provision of such assistance.

5.2 Notification Obligations. Company shall, to the extent legally permitted, promptly notify Customer if it receives a request from a Data Subject for access to, correction, amendment, deletion of, or objection to the Processing of Customer Personal Data relating to such individual. Company shall not respond to any such Data Subject request relating to Customer Personal Data without Customer's prior written consent except to confirm that the request relates to Customer. Furthermore, Company shall, to the extent legally permitted, promptly notify Customer if it receives a request for disclosure of or correspondence, notice or other communication relating to Customer Personal Data from law enforcement, a competent authority, or a relevant data protection authority. Company shall provide Customer with appropriate reasonable cooperation and assistance in relation to handling any such request, to the extent legally permitted and to the extent Customer does not have access to such Customer Personal Data through its use or receipt of the Products and/or Services. If legally permitted, Customer shall be responsible for any cost arising from Company's provision of such assistance.

6. Personal Data Breach

6.1 Notification Obligations. In the event Company becomes aware of a verified Security Breach, Company will notify Customer of the Security Breach without undue delay and in any event no later than seventy-two (72) hours of discovery. The obligations in this Section 6 do not apply to incidents that are caused by Customer or Customer's personnel or end users or to unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

6.2 Manner of Notification. Notification of Security Breaches, if any, will be delivered to Customer's GDPR point of contact via e-mail or over the telephone. It is Customer's sole responsibility to ensure it maintains accurate contact information on Company's support systems at all times.

6.3 Content of Notification. Where notification is required, such notification shall at a minimum:

6.3.1 describe the nature of the Security Breach, the categories and numbers of Data Subjects concerned, and the categories and numbers of Personal Data records concerned;

6.3.2 communicate the name and contact details of Company's relevant contact from whom more information may be obtained;

6.3.3 describe the likely consequences of the Security Breach; and

6.3.4 describe the measures taken or proposed to be taken to address the Security Breach.

7. Deletion or Return of Customer Personal Data

7.1 Delete or Return. Subject to section 7.3, Company agrees to promptly and in any event within thirty (30) days of the date of cessation of any services involving the Processing of Customer Personal Data (the "**Cessation Date**"), securely delete Customer Personal Data or, at Customer's timely written request, return a complete copy of any and all Customer Personal Data to Customer by secure file transfer in such format as is reasonably requested by Customer.

7.2 Definition of Delete. For clarification, "**Delete**" means to remove or obliterate Personal Data such that it cannot be recovered or reconstructed.

7.3 Records. Company may retain Customer Personal Data to the extent required by Applicable Laws or as mandated in Company's document retention schedule, provided that Company shall ensure the confidentiality of all such Customer Personal Data.

8. Audit rights

8.1 Audit Rights. No more than once per year, Customer may engage a mutually agreed upon third party to audit Company solely for the purposes of meeting its audit requirements pursuant to Article 28, Section 3(h) of the GDPR. To request an audit, Customer must submit a detailed audit plan at least four (4) weeks in advance of the proposed audit date describing the proposed scope, duration, and start date of the audit. Audit requests must be sent to privacy@commandalkon.com. The auditor must execute a written confidentiality agreement acceptable to Company before conducting the audit. The audit must be conducted during regular business hours, subject to Company's policies, and may not unreasonably interfere with Company's business activities. Any audits are at Customer's sole cost and expense. Company will cooperate with any Customer or any competent regulatory or supervisory authority audit request to verify Company's compliance with its obligations under this DPA by making available, subject to non-disclosure obligations, third party audit reports, where available, descriptions of security controls and other information reasonably requested by Customer regarding Company's security practices and policies.

8.2 Compliance Assistance. Taking into account the nature of the Processing and the information available to Company, Company will provide adequate reasonable cooperation and assistance to Customer regarding Customer's compliance obligations described in Articles 32-36 of the GDPR.

9. Data Transfers

9.1 General Authorization. Customer agrees that Company may, subject to Section 9.2, store and Process Customer Personal Data in the United States of America and any other country in which Company or any of its sub-processors maintains facilities or otherwise Processes Personal Data. Any such transfers shall be governed by Company's inter-affiliate Standard Contractual Clauses or Company's Privacy Shield certification (should it be reinstated). Company will not transfer, or cause to be transferred, any Customer Personal Data from one jurisdiction to another unless in accordance with applicable law and will not cause Customer to be in breach of any Data Protection Law.

9.2 Standard Contractual Clauses. To the extent, and only to the extent, Company Processes Customer Personal Data from the European Economic Area, Switzerland, or the UK and Standard Contractual Clauses are required, the applicable Standard Contractual Clauses (EEA or UK) shall apply and are hereby incorporated. For purposes of the Standard Contractual Clauses, Customer is the "data exporter" and Company is the "data importer." Company has the 2021 Standard Contractual Clauses in place between Company affiliates and has maintained self-certification to the Privacy Shield (in case it is reinstated) for purposes of data transfers to the United States of America.

9.3 UK Standard Contractual Clauses. The parties agree that the UK Standard Contractual Clauses will apply to personal data that is transferred via the products and/or services from the United Kingdom, either directly or via onward transfer, to any country or recipient outside of the United Kingdom that is not recognized by the competent United Kingdom regulatory authority or governmental body for the United Kingdom as providing an adequate level of protection for personal data. For data transfers from the United Kingdom that are subject to the UK Standard Contractual Clauses, the UK Standard Contractual Clauses will be deemed entered into (and incorporated into this Addendum by this reference).

9.4 Supplemental Measures. In supplement to the Standard Contractual Clauses, if Company becomes aware that any governmental authority (including law enforcement) wishes to obtain access to or a copy of some or all of the Customer Personal Data processed by Company, whether on a voluntary or a mandatory basis, for purposes related to national security intelligence, then unless legally prohibited or under a mandatory legal compulsion that requires otherwise, Company will: 1) immediately notify the Customer to whom the personal data applies; 2) inform the relevant government authority that it has not been authorized to disclose the Customer Personal Data and, unless legally prohibited, will need to immediately notify the Customer to whom the Customer Personal Data applies; 3) inform the governmental authority that it should direct all requests or demands directly to the Customer to whom the Customer Personal Data applies; and 4) not provide access to the Customer Personal Data until authorized in writing by the Customer to whom the Customer Personal Data applies or until compelled legally to do so. If legally compelled to do so, Company will use reasonable and lawful efforts to challenge such prohibition or compulsion. If Company is compelled to produce the Customer Personal Data, Company will only disclose Customer Personal Data to the extent legally required to do so in accordance with applicable lawful process.

9.5 Transfer Precedence. In the event that services are covered by more than one transfer mechanism, the transfer of Customer's Personal Data will be subject to a single transfer mechanism in accordance with the following order of precedence: (i) EU Standard Contractual Clauses (where required by applicable Data Protection Law); (ii) Privacy Shield self-certification (should it be reinstated).

10. Term and Termination

Term of DPA. This DPA will take effect on the date on which it is fully executed and, notwithstanding expiry of the term of any purchased subscription, remain in effect until, and automatically expire upon, deletion of all Customer Personal Data as described in this DPA.

11. Noncompliance; Remedies; Parties

11.1 Limitation of Liability. Company’s liability for breach of its obligations in this DPA are subject to the limitation of liability provision in the Agreement.

11.2 Parties to this DPA. Nothing in the DPA shall confer any benefits or rights on any person or entity other than the parties to this DPA.

12. General Terms

Governing law and jurisdiction

12.1 This DPA will be reviewed one year from date of issue and then three years thereafter, or sooner if appropriate.

12.2 Unless required by the Standard Contractual Clauses:

12.2.1 the parties to this Addendum hereby submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this Addendum, including disputes regarding its existence, validity or termination; and

12.2.2 this Addendum and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Agreement.

Order of precedence

12.3 In the event of any conflict or inconsistency between this Addendum and the Standard Contractual Clauses where the Standard Contractual Clauses are required, the Standard Contractual Clauses shall prevail.

12.4 Subject to section 12.2, with regard to the subject matter of this Addendum, in the event of inconsistencies between the provisions of this Addendum and any other agreements between the parties, including the Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this Addendum, the provisions of this Addendum shall prevail.

Changes in Data Protection Laws

12.5 Customer may:

12.5.1 by at least thirty (30) calendar days' written notice to Company from time to time propose any variations to the Standard Contractual Clauses which are required as a result of any change in, or decision of a competent authority under, that Data Protection Law; and

12.5.2 propose any other variations to this Addendum which Customer reasonably considers to be necessary to address the requirements of any Data Protection Law.

12.6 If Customer gives notice under section 12.5 the parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in Customer's notice as soon as is reasonably practicable.

Severance

12.7 Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either: (i) amended as necessary to ensure its validity and enforceability, while preserving the parties’ intentions as closely as possible or, if this is not possible; (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

ANNEX I TO STANDARD CONTRACTUAL CLAUSES

A. LIST OF PARTIES

Data exporter(s)[1]: [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Name:

Address:

Contact person's name, position and contact details:

Activities relevant to the data transferred under these Clauses:

Signature and date:

Role: Controller

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Name: Command Alkon Incorporated

Address: 1800 Industrial Park Drive, Suite 400, Birmingham, Alabama 35243 USA

Contact person's name, position and contact details: David R. Burkholder, Associate General Counsel and Chief Privacy Officer, dburkholder@commandalkon.com, 1-205-263-5524 ext. 2837

Activities relevant to the data transferred under these Clauses:

Chief Privacy Officer for compliance purposes

Signature and date:

Role: Processor

[1] If this section is not completed, the Data Exporter will be the entity identified in the associated Master License and Services Agreement and associated documents.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Employees of Customer; customers of Customer; employees of business affiliates of Customer.

Categories of personal data transferred

Contact information; website, product, and service interaction information; addresses; date of birth; location of birth; e-mail addresses; names; gender; title; telephone numbers; driver’s license number; signature; employee number; geo-location information; pay rate; username; password; performance information; qualifications and restrictions.

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 specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures

No sensitive data as defined by the GDPR is transferred.

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

Continuous transfer of data as the product/platform is used by the end users.

Nature of the processing

As necessary for provision of the product/service under the Agreement and as instructed by the Exporter.

Purpose(s) of the data transfer and further processing

As necessary for provision of the product/service or in support of the product/service.

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

For the period required to provide the product/service and in conjunction with the Company data retention policy and schedule or as required by applicable law or regulation.

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

For support required to provide the product/service (i.e., cloud storage services) and for the period required to provide the product/service.

C. COMPETENT SUPERVISORY AUTHORITY

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

Data Protection Authority of the Netherlands.

ANNEX II TO STANDARD CONTRACTUAL CLAUSES

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

Description of the technical and organisational 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.

Measures of pseudonymisation and encryption of personal data **Encryption in transit and at rest is implemented**

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services **Command Alkon governs itself under the NIST 800-171 security framework, as well as the AWS CIS Benchmarks v1.2 and AWS Foundational Best Practices v1.0**

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident **Command Alkon conducts regular scheduled backups and high availability patterned architecture is utilized**

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing **Automated regular vulnerability testing; annual penetration testing; annual privacy and security audits**

Measures for user identification and authorization **Multi-factor authentication; sophisticated password program; permissions limitations; logging**

Measures for the protection of data during transmission **Encryption in transit**

Measures for the protection of data during storage **Encryption at rest; logical access controls; redundancy via backup and failover**

Measures for ensuring physical security of locations at which personal data are processed **Key cards/codes; visitor registration; security video; security officers; security/privacy training**

Measures for ensuring events logging **Logging in place and monitored; logging is fed to a managed third-party service; event alerts turned on**

Measures for ensuring system configuration, including default configuration **All configuration states and changes are tracked; change management program implemented**

Measures for internal IT and IT security governance and management **Security and privacy policies and procedures; Chief Information Security Officer; dedicated SecOps team; Chief Privacy Officer; security/privacy training**

Measures for certification/assurance of processes and products **NIST 800-171; CIS AWS Benchmark v1.2; AWS Foundational Best Practices v1.0**

Measures for ensuring data minimization **Data processed is only by fields entered by the end users/customer/Controller**

Measures for ensuring data quality **Data processed is entered and maintained by the end users/customer/Controller**

Measures for ensuring limited data retention **Data retention is controlled by contractual obligations and the data retention policy and schedule**

Measures for ensuring accountability **Accountability is addressed through monitored logging; logging is fed to a managed third-party service; event alerts turned on**

Measures for allowing data portability and ensuring erasure **Data portability is handled on a case-by-case basis and erasure is ensured through contractual obligations and notice-and-confirmation processes**

For transfers to (sub-) processors, also describe the specific technical and organisational 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

Sub-processors who process personal data are subject to contractual restrictions and Data Processing Addenda requiring compliance with the Standard Contractual Clauses where required