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 THE DATA PROTECTION ADDENDUM

STANDARD CONTRACTUAL CLAUSES

Adopted by the European Commission in Implementing Decision (EU) 2021/914, 4 June 2021

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 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) 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

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.

8.1 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.

8.2 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.

8.3 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 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.

8.4 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.

8.5 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).

8.6 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.

8.7 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.

8.8 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 ([1]) (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.

8.9 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

[1] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

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) GENERAL WRITTEN AUTHORISATION. The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least ten (10) business days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(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. ([2]) The Parties agree that, by complying with this Clause, the data importer fulfils 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 fulfil its obligations under that contract.

[2] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

(e) The data importer shall agree to 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) 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.

(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

(a) 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.

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

(i) 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;

(ii) 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 ([3]);

(iii) 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.

(c) 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.

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

(e) 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).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil 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.

[3] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 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.

15.2 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.

ANNEX I TO STANDARD CONTRACTUAL CLAUSES

A. LIST OF PARTIES

Data exporter(s)[4]: [*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

[4] 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