DATA PROCESSING ADDENDUM
(Rev.6 March 2023)

This Data Processing Addendum ("DPA") forms part of the Master Subscription Agreement or other written or electronic agreement between FinancialForce ("FF") and Customer for the purchase of online services (including associated FF offline or mobile components) from FF (identified either as "Services" or otherwise in the applicable agreement, and hereinafter defined as "Services") (the "Agreement") to reflect the parties' agreement with regard to the Processing of Personal Data.
By signing the Agreement, Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws and Regulations, in the name and on behalf of its Authorized Affiliates, if and to the extent FF processes Personal Data for which such Authorized Affiliates qualify as the Controller. For the purposes of this DPA only, and except where indicated otherwise, the term "Customer" shall include Customer and Authorized Affiliates. All capitalised terms not defined herein shall have the meaning set forth in the Agreement.
In the course of providing the Services to Customer pursuant to the Agreement, FF may Process Personal Data on behalf of Customer. FF agrees to comply with the following provisions with respect to any Personal Data submitted by or for Customer to the Services, collected by or for Customer using the Services and/or and Processed in the provision of the Services.

To complete this DPA, Customer must send the completed and signed DPA and SCCs to FF at privacy@financialforce.com.

HOW THIS DPA APPLIES

If the Customer entity signing this DPA is a party to the Agreement, this DPA is an addendum to and forms part of the Agreement. In such case, the FF entity that is party to the Agreement is party to this DPA. If the Customer entity signing this DPA has executed an Order Form with FF or its Affiliate pursuant to the Agreement, but is not itself a party to the Agreement, this DPA is an addendum to that Order Form and applicable renewal Order Forms, and the FinancialForce entity that is party to such Order Form is party to this DPA. If the Customer entity signing this DPA is neither a party to an Order Form nor the Agreement, this DPA is not valid and is not legally binding. Such entity should request that the Customer entity that is a party to the Agreement execute this DPA.

This DPA shall not replace any comparable or additional rights relating to Processing of Customer Data contained in Customer's Agreement (including any existing data processing addendum to the Agreement).

1. DEFINITIONS

"Approved Jurisdiction" means a member state of the EEA, or other jurisdiction approved as having adequate legal protections for data by the European Commission, currently found here: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-dataprotection/adequacy-decisions_en.

"Authorized Affiliate" means any of Customer's Affiliate(s) which (a) is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Services pursuant to the Agreement between Customer and FF, but has not signed its own Order Form with FF and is not a "Customer" as defined under the Agreement.

"CCPA" means the California Consumer Privacy Act Cal. Civ. Code § 1798.100 et seq. and its implementing regulations.

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

"Customer Data" means what is defined in the Agreement as "Customer Data" or "Your Data".

"Data Protection Laws and Regulations" means all mandatory laws and regulations as applicable to the Processing of Personal Data hereunder.

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

"Effective Date" means the last date beneath the parties' signatures below.

"FF" means the FinancialForce entity which is a party to the Agreement.

"FF Group" means FF and its Affiliates engaged in the Processing of Personal Data.

"GDPR" means the 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

"Personal Data" means any information relating to (i) an identified or identifiable natural person or household, and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data, personal information or personally identifiable information under applicable Data Protection Laws and Regulations), where for each (i) or (ii), such data is Customer Data where processed in accordance with this DPA.

"Processing" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. For the avoidance of doubt, "process" and "processed" will be interpreted accordingly.

"Processor" means the entity which processes Personal Data on behalf of the Controller including as applicable any "service provider" as that term is defined by the applicable Data Protection Laws and Regulations.

"**Standard Contractual Clauses**" means either the standard contractual clauses approved by the European Commission for the transfer of Personal Data to processors or those for the transfer of Personal Data to controllers in each case established in third countries which do not ensure an adequate level of data protection and any subsequent changes approved by the European Commission with an official decision.

"Sub-processor" means any Processor engaged by FF, (including any other member of the FF Group), engaged or permitted by FF to process Personal Data under this DPA.

"Supervisory Authority" means an independent public authority which is established by an EU Member State pursuant to the GDPR or by the applicable Data Protection Laws and Regulations in the EEA, Switzerland and the UK.

"UK GDPR" means the GDPR as transposed into United Kingdom national law by operation of section 3 of the European Union (Withdrawal) Act 2018, as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019. In this DPA, in circumstances where the UK GDPR applies, references to the GDPR and its provisions will be construed as references to the UK GDPR and its corresponding provisions, and references to EU or Member State law shall be construed as references to UK law.

2. PROCESSING OF PERSONAL DATA

2.1. Roles of the Parties. The parties acknowledge and agree that with regard to the Processing of Personal Data in the course of providing the Services to Customer pursuant to the Agreement, Customer is the Controller, FF is a Processor and that FF will engage Sub-processors, including other members of the FF Group, pursuant to clause 5 "Sub-processors" below.

2.2. Customer's Processing of Personal Data. Customer shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations including any applicable requirement to provide notice to Data Subjects of the use of FF as Processor. For the avoidance of doubt, Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data. Customer represents that its use of the Services will not violate the rights of any Data Subject that has opted-out from the sale of or other disclosure of Personal Data, to the extent applicable under the CCPA, nor shall the use of the Services violate any rights of any Data Subject to the extent applicable under the Data Protection Laws and Regulations.

2.3. FF's Processing of Personal Data. FF shall treat Personal Data as Confidential Information and shall (i) only Process Personal Data on behalf of and in accordance with Customer's instructions for the following purposes: (a) Processing in accordance with the Agreement and applicable Order Form(s); (b) Processing initiated by Users in their use of the Services; and (c) Processing to comply with other reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement; and (ii) process Personal Data in accordance with this DPA. FF is prohibited from: (i) selling the Personal Data; (ii) retaining, using, disclosing, or Processing Personal Data for any purpose other than for the specific purpose of performing the Services specified

in the Agreement; including retaining, using, or disclosing the Personal Data for a commercial purpose other than providing the Services specified in the Agreement; or (iii) retaining, using, or disclosing the Personal Data outside of the direct business relationship between Customer and FF;. FF hereby confirms that it understands the restrictions set forth in this section and will comply with them.

2.4. **Details of the Processing.** The subject-matter of Processing of Personal Data by FF is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Attachment 1 (Details of the Processing) to this DPA.

3. RIGHTS OF DATA SUBJECTS

3.1. **Data Subject Request.** FF shall, to the extent legally permitted, promptly notify Customer if FF receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making ("Data Subject Request"). Taking into account the nature of the Processing, FF shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, FF shall upon Customer's request use commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent FF is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, Customer shall be responsible for any costs arising from FF's provision of such assistance.

4. FF PERSONNEL

4.1. **Confidentiality.** FF shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements. FF shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

4.2. **Reliability.** FF shall take commercially reasonable steps to ensure the reliability of any FF personnel engaged in the Processing of Personal Data.

4.3. **Limitation of Access.** FF shall ensure that FF's access to Personal Data is limited to those personnel who require such access to perform the Agreement.

4.4. **Data Protection Officer.** Members of the FF Group will appoint a data protection officer where such appointment is required by Data Protection Laws and Regulations. The appointed person may be reached at privacy@financialforce.com.

5. SUB-PROCESSORS

5.1. **Appointment of Sub-processors.** Customer acknowledges and agrees that (a) members of the FF Group may be retained as Sub-processors; (b) FF and FF's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services; and (c) Salesforce and members of the Salesforce Group may be retained as Sub-processors. FF or a FF Affiliate shall enter into a written agreement with each Sub-processor containing data protection obligations not less protective than those in this DPA with respect to the protection of Customer Data to the extent applicable to the nature of the services provided by such Sub-processor.

5.2. **List of Current Sub-processors and Notification of New Sub-processors.** A current list of Sub-processors for the Services, including the identities of those Sub-processors and their country of location, is accessible here **("Sub-processor Lists")**. Customer may receive notifications of new Sub-processors and updates to existing Sub-Processor by subscribing for updates and if a Customer contact subscribes, FF shall provide the subscriber with notification of new Sub-processor(s) before authorizing such new Sub-processor(s) to Process Personal Data in connection with the provision of the applicable Services.("**Updated Sub-processor List**").

5.3. **Objection Right for New Sub-processors.** Customer may object to FF's use of a new Sub-processor by notifying FF in writing within ten (10) business days after receipt of an Updated Sub-processor List. In the event Customer objects to a new Sub-processor, as permitted in the preceding sentence, FF will use commercially reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-

processor without unreasonably burdening the Customer. If FF is unable to make available such change within a reasonable period of time, which shall not exceed sixty (60) days, Customer may terminate the applicable Order Form(s) with respect only to those Services which cannot be provided by FF without the use of the objected-to new Sub-processor, by providing written notice to FF. FF will refund to Customer any prepaid fees covering the remainder of the term of such Order Form(s) following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on Customer.

5.4. **Liability.** FF shall be liable for the acts and omissions of its Sub-processors to the same extent FF would be liable if performing the services of each Sub-processor directly under the terms of this DPA, save as otherwise set forth in the Agreement.

6. SECURITY

6.1. **Controls for the Protection of Personal Data.** FF shall maintain administrative, physical and technical safeguards designed for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Customer Data), confidentiality and integrity of Customer Data, including Personal Data, in accordance with Annex 2 to the Standard Contractual Clauses. FF will not materially decrease the overall security of the Services during a subscription term.

6.2. **Attestations/Certifications.** Upon Customer's written request no more frequently than once annually, FF shall provide to Customer a copy of FF's then most recent security attestations and/or certification(s) in place for the Services e.g. a SOC1 or SOC 2 report. FF may require Customer to sign a nondisclosure agreement reasonably acceptable to FF before FF provides a copy of such security attestations/ certification(s) to Customer.

7. SECURITY BREACH MANAGEMENT AND NOTIFICATION

7.1. FF maintains security incident management policies and procedures and shall notify Customer without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data, including Personal Data, transmitted, stored or otherwise Processed by FF or its Sub-processors of which FF becomes aware (a "Customer Data Incident"). FF shall make reasonable endeavours to identify the cause of such Customer Data Incident and take those steps as FF deems necessary and reasonable in order to remediate the cause of such a Customer Data Incident to the extent the remediation is within FF's reasonable control. The obligations herein shall not apply to incidents that are caused by Customer or Customer's Users.

8. RETURN AND DELETION OF CUSTOMER DATA

8.1. FF shall return Customer Data to Customer and, to the extent allowed by applicable law, delete Customer Data in accordance with the procedures and timeframes specified in the Agreement and Trust and Compliance Documentation (Security, Privacy and Architecture).

9. AUTHORIZED AFFILIATES

9.1. **Contractual Relationship.** The parties acknowledge and agree that, by executing the Agreement, Customer enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, thereby establishing a separate DPA between FF and each such Authorized Affiliate subject to the provisions of the Agreement, this Clause 9, and Clause 10 below. Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, an Authorized Affiliate is not and does not become a party to the Agreement, and is only a party to the DPA. All access to and use of the Services by Authorized Affiliates must comply with the terms and conditions of the Agreement, and any violation of the terms and conditions of the Agreement by an Authorized Affiliate shall be deemed a violation by Customer.

9.2. **Communication.** The Customer that is the contracting party to the Agreement shall remain responsible for coordinating all communication with FF under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

9.3. **Rights of Authorized Affiliates.** Where an Authorized Affiliate becomes a party to the DPA with FF, it shall to the extent required under applicable Data Protection Laws and Regulations be entitled to exercise the rights and seek remedies under this DPA, subject to the following:

9.3.1. Except where applicable Data Protection Laws and Regulations require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against FF directly by itself, the parties agree that (i) solely the Customer that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (ii) the Customer that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Authorized Affiliate individually but in a combined manner for all of its Authorized Affiliates together (as set forth, for example, in Clause 9.3.2, below).

9.3.2. The Customer that is the contracting party to the Agreement shall, when carrying out an on-site audit of the procedures relevant to the protection of Personal Data, take all reasonable measures to limit any impact on FF and its Sub-Processors by combining, to the extent reasonable possible, several audit requests carried out on behalf of different Authorized Affiliates in one single audit.

10. LIMITATION OF LIABILITY

10.1. Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and FF, whether in contract, tort or under any other theory of liability, is subject to the "Limitation of Liability" clause of the Agreement, and any reference in such clause to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together.

For the avoidance of doubt, FF's and its Affiliates' total liability for all claims from the Customer and all of its Authorized Affiliates arising out of or related to the Agreement and each DPA shall apply in the aggregate for all claims under both the Agreement and all DPAs established under this Agreement, including by Customer and all Authorized Affiliates, and, in particular, shall not be understood to apply individually and severally to Customer and/or to any Authorized Affiliate that is a contractual party to any such DPA. Also for the avoidance of doubt, each reference to the DPA in this DPA means this DPA including its Schedules and any Appendices thereto.

11. TRANSFERS OF PERSONAL DATA

11.1. **Transfers of Personal Data from EEA or Switzerland to third countries.** Where FF Processes Personal Data from the EEA or Switzerland on behalf of Customer, in a country which is not an Approved Jurisdiction, FF shall perform such Processing in accordance with the Standard Contractual Clauses set forth in Attachment 2 to this DPA and/or in accordance with Articles 44 to 49 of the GDPR.

11.2. **Transfers of Personal Data from the UK to third countries.** Where FF Processes Personal Data from the UK in a third country, such Processing shall be performed in accordance with Attachment 2, as amended by the UK Addendum to the EU Commission Standard Contractual Clauses included in (the "Addendum") and/or in accordance with the UK GDPR. Any further changes to this Addendum approved with an official decision by the Information Commissioner's Office will be incorporated by reference and a copy of the new Addendum will be available on the FF Privacy Webpage.

11.3. In the event that the form of the Standard Contractual Clauses referred to in this Clause 11 is changed or replaced by the relevant authorities under Data Protection Laws and Regulations, the Customer as Controller should notify FF as Processor of such form. Provided that such form is accurate and applicable to FF as Processor, such form shall then be binding upon the parties when both parties have executed the revised form, subject to the expiration of a grace period, if any, determined by the relevant Supervisory Authorities.

11.4. **Data Protection Impact Assessment.** Upon Customer's request, FF shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligation under the GDPR and/or UK GDPR (as applicable) to carry out a data protection impact assessment related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to FF. FF shall provide reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to this Clause 11.4, to the extent required under the GDPR and/or UK GDPR (as applicable).

11.5. FF will not disclose Customer Data to a law enforcement agency unless required by law. If a law enforcement agency contacts FF with a demand for Customer Data, FF will attempt to redirect the law enforcement agency to request that data directly from Customer. If compelled to disclose Customer Data to a law enforcement agency, FF will promptly notify Customer and provide a copy of the demand unless legally prohibited from doing so. Upon receipt of any other third-party request for Customer Data, FF will promptly notify Customer unless prohibited by law. FF will reject the request unless required by law to comply. If the request is valid, FF will attempt to redirect the third party to request the data directly from Customer. FF will not provide any third party: (a) direct, indirect, blanket, or unfettered access to Customer Data; (b) platform encryption keys used to secure Customer Data or the ability to break such encryption; or (c) access to Customer Data if FF is aware that the data is to be used for purposes other

than those stated in the third party's request. In support of the above, FF may provide Customer's basic contact information to the law enforcement agency or third party, as applicable. FF will document and record the requests for access received from public authorities and the response provided, alongside a summary of the legal reasoning and the actors involved. When and to the extent legally permissible, FF will provide these records to Customer, who may provide them to affected Data Subjects.

12. Audit

12.1. Upon Customer's request, and subject to the confidentiality obligations set forth in the Agreement, FF shall make available to Customer (or Customer's independent, third-party auditor that is not a competitor of FF and that has signed nondisclosure agreement reasonably acceptable to FF) information regarding the FF Group's compliance with the obligations set forth in this DPA in the form of FF's SOC 1 or SOC 2 report and, for its Sub-processors salesforce.com, inc. and its subsidiaries, the third-party certifications and audits set forth in the Salesforce.com Security, Privacy and Architecture Documentation located at to the extent Salesforce makes them generally available to its customers. Following any notice by FF to Customer of an actual or reasonably suspected unauthorized disclosure of Personal Data, upon Customer's reasonable belief that FF is in breach of its obligations in respect of protection of Personal Data under this DPA, or if such audit is required by Customer's Supervisory Authority, Customer may contact FF in accordance with the "Notices" Clause of the Agreement to request an audit at FF's premises of the procedures relevant to the protection of Personal Data. Any such request shall occur no more than once annually, save in the event of an actual or reasonably suspected unauthorised access to Personal Data. Customer shall reimburse FF for any time expended for any such on-site audit at the FF Group's then-current professional services rates, which shall be made available to Customer upon request. Before the commencement of any such on-site audit, Customer and FF shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by FF. Customer shall promptly notify FF with information regarding any non-compliance discovered during the course of an audit.

12.2. **Conflict.** In the event of any conflict or inconsistency between the body of this DPA and any of its Schedules (not including the Standard Contractual Clauses) and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

The parties' authorized signatories have duly executed this Agreement:

CUSTOMER	**FINANCIALFORCE.COM INC.**
Signed: _____	Signed: DocuSigned by: Judith Kirkpatrick CD24F5D52D2843C...
Name: _____	Name: Judith Kirkpatrick
Title: _____	Title: Associate General Counsel

List of Schedules

Attachment 1: Details of the Processing

Attachment 2: Controller to Processor Standard Contractual Clauses

Attachment 3: International Data Transfer Addendum to the EU Commission SCCs

Attachment 1

Details of the Processing

Nature and Purpose of Processing

FF will Process Personal Data as necessary to perform the Services pursuant to the Agreement, as further specified in the Documentation, and as further instructed by Customer in its use of the Services.

Duration of Processing

Subject to Clause 8 of the DPA, FF will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

Categories of Data Subjects

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Prospects, customers, business partners, vendors and subcontractors of Customer (who are natural persons)
- Employees or contact persons of Customer's customers, business partners, vendors and subcontractors
- Employees, agents, advisors, contractors, and freelancers of Customer (who are natural persons), and their family members
- Customer's Users authorized by the data exporter to use the Services

Type of Personal Data

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- First and last name
- Title
- Position
- Employer
- Contact information (company, email, phone, physical business address)
- ID data
- Professional life data
- Professional skills information
- Personal life data
- Health and medical information
- Compensation information
- Connection data
- Localisation data

Attachment 2

Controller to Processor SCCs

SECTION 1

1. **PURPOSE AND SCOPE**

1.1 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 personal data to a third country.

1.2 The Parties:

1.2.1 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 1.A** (hereinafter each 'Data Exporter'); and

1.2.2 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 1.A** (hereinafter each 'Data Importer')

have agreed to these standard contractual clauses (hereinafter: 'clauses').

1.3 These clauses apply with respect to the transfer of personal data as specified in **Annex 1.B**.

1.4 The Appendix to these clauses containing the Annexes referred to therein forms an integral part of these clauses.

2. **EFFECT AND INVARIABILITY OF THE CLAUSES**

2.1 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.

2.2 These clauses are without prejudice to obligations to which the Data Exporter is subject by virtue of Regulation (EU) 2016/679.

3. **THIRD-PARTY BENEFICIARIES**

3.1 Data subjects may invoke and enforce these clauses, as third-party beneficiaries, against the Data Exporter and/or Data Importer, with the following exceptions:

3.1.1 **clause 1**, **clause 2**, **clause 3**, **clause 6**, **clause 7**;

3.1.2 **clause 8.1.2**, **8.9.1**, **8.9.3**, **8.9.4** and **8.9.5**;

3.1.3 **clause 9.1**, **9.3**, **9.4** and **9.5**;

3.1.4 **clause 12.1**, **12.4** and **12.1**;

3.1.5 **clause 13**;

3.1.6 **clause 15.1.3**, **15.1.4** and **15.1.5**;

3.1.7 **clause 16.5**;

3.1.8 **clause 18.1** and **18.2**.

3.2 **Clause 3.1** is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

4. **INTERPRETATION**

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

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

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

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.

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 1.B**.

7. **DOCKING CLAUSE**

7.1 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 1.A**.

7.2 Once it has completed the Appendix and signed **Annex 1.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 1.A**.

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

SECTION 2 – OBLIGATIONS OF THE PARTIES

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**

8.1.1 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.

8.1.2 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 1.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 2** and personal data, the Data Exporter may redact part of the text of the **Appendix** to these clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This clause is without prejudice to the obligations of the Data Exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

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 1.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 14.5** 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 14.1**.

8.6 **Security of processing**

8.6.1 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 2**. The Data Importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

8.6.2 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.

8.6.3 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.

8.6.4 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 1.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 (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:

8.8.1 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;

8.8.2 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;

8.8.3 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

8.8.4 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**

8.9.1 The Data Importer shall promptly and adequately deal with enquiries from the Data Exporter that relate to the processing under these clauses.

8.9.2 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.

8.9.3 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.

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

8.9.5 The Parties shall make the information referred to in **clauses 8.9.2** and **8.9.3**, including the results of any audits, available to the competent supervisory authority on request

9. **USE OF SUB-PROCESSORS**

9.1 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 10 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.

9.2 Where the Data Importer engages a sub-processor to carry out specific processing activities (on behalf of the Data Exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the Data Importer under these clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this clause, the Data Importer 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.

9.3 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.

9.4 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.

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

10. **DATA SUBJECT RIGHTS**

10.1 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.

10.2 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 2** 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.

10.3 In fulfilling its obligations under **clauses 10.1** and **10.2**, the Data Importer shall comply with the instructions from the Data Exporter.

11. **REDRESS**

11.1 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.

11.2 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.

11.3 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:

11.3.1 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**;

11.3.2 refer the dispute to the competent courts within the meaning of **clause 18**.

11.4 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.

11.5 The Data Importer shall abide by a decision that is binding under the applicable EU or Member State law.

11.6 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.

12. **LIABILITY**

12.1 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.

12.2 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.

12.3 Notwithstanding **clause 12.2**, 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.

12.4 The Parties agree that if the Data Exporter is held liable under **clause 12.3 f**or 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.

12.5 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.

12.6 The Parties agree that if one Party is held liable under **clause 12.5**, 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.

12.7 The Data Importer may not invoke the conduct of a sub-processor to avoid its own liability.

13. **SUPERVISION**

13.1 Where the Data Exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the Data Exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in **Annex 1.C**, shall act as competent supervisory authority.

Where the Data Exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which

the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in **Annex 1.C**, shall act as competent supervisory authority.

Where the Data Exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in **Annex 1.C**, shall act as competent supervisory authority.

13.2 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 3 – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

14. LOCAL LAWS AND PRACTICES AFFECTING COMPLIANCE WITH THE CLAUSES

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

14.2 The Parties declare that in providing the warranty in **clause 14.1**, they have taken due account in particular of the following elements:

14.2.1 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;

14.2.2 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;

14.2.3 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.

14.3 The Data Importer warrants that, in carrying out the assessment under **clause 14.2**, 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.

14.4 The Parties agree to document the assessment under **clause 14.2** and make it available to the competent supervisory authority on request.

14.5 The Data Importer agrees to notify the Data Exporter promptly if, after having agreed to these clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under **clause 14.1**, 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 **clause 14.1**.

14.6 Following a notification pursuant to **clause 14.5,** 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 16.4** and **16.5** shall apply.

15. **OBLIGATIONS OF THE DATA IMPORTER IN CASE OF ACCESS BY PUBLIC AUTHORITIES**

15.1 **Notification**

15.1.1 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:

15.1.1.1 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

15.1.1.2 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.

15.1.2 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.

15.1.3 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.).

15.1.4 The Data Importer agrees to preserve the information pursuant to **clauses 15.1.1** to **15.1.3** for the duration of the contract and make it available to the competent supervisory authority on request.

15.1.5 **Clauses 15.1.1** to **15.1.3** are without prejudice to the obligation of the Data Importer pursuant to **clause 14.5** 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**

15.2.1 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 14.5**.

15.2.2 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.

15.2.3 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 4 – FINAL PROVISIONS

16. NON-COMPLIANCE WITH THE CLAUSES AND TERMINATION

16.1 The Data Importer shall promptly inform the Data Exporter if it is unable to comply with these clauses, for whatever reason.

16.2 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 14.6**.

16.3 The Data Exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these clauses, where:

16.3.1 the Data Exporter has suspended the transfer of personal data to the Data Importer pursuant to **clause 16.2** and compliance with these clauses is not restored within a reasonable time and in any event within one month of suspension;

16.3.2 the Data Importer is in substantial or persistent breach of these clauses; or

16.3.3 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.

16.4 Personal data that has been transferred prior to the termination of the contract pursuant to **clause 16.3** 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.

16.5 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.

17. GOVERNING LAW

These clauses shall be governed by the law of one of the EU Member States, provided such law allows for third- party beneficiary rights. The Parties agree that this shall be the law of The Netherlands

18. **CHOICE OF FORUM AND JURISDICTION**

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

18.2 The Parties agree that those shall be the courts of Amsterdam.

18.3 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.

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

APPENDIX

EXPLANATORY NOTE:

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

Annex 1

A. **LIST OF PARTIES**

Data exporter(s): 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 [DATA EXPORTER TO COMPLETE]

Name: . . . . . .

Address: . . . . . .

Contact person's name, position and contact details: . . . . . .

Activities relevant to the data transferred under these clauses: . . . . . .

Signature and date: . . . . . .

Role (controller/processor): . . . . . .

[PLEASE REPLICATE SECTION ABOVE IF THERE ARE MULTIPLE EXPORTERS]

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

Name: FinancialForce.com, Inc.

Address: 60 South Market Street, Suite 750, San Jose, CA 95113.

Contact person's name, position and contact details: Privacy Officer, privacy@financialforce.com

Activities relevant to the data transferred under these clauses: FinancialForce.com, Inc. is a provider of enterprise cloud computing solutions.

Signature and date: . . . DocuSigned by: Judith Kirkpatrick CD24F5D52D2843C... March 15, 2023 . . . .

Role (controller/processor): Processor

[REPLICATE SECTION ABOVE IF THERE ARE MULTIPLE IMPORTERS]

B. **DESCRIPTION OF TRANSFER**

Categories of data subjects whose personal data is transferred

The personal data transferred concern the following categories of data subjects (please specify):

Data exporter may submit personal data in connection with the provision of technical support or consulting services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to personal data concerning the following categories of data subjects (please specify):

- Prospects, customers, business partners, vendors and subcontractors of the data exporter (who are natural persons)
- Employees or contact persons of the data exporter's customers, business partners, vendors and subcontractors

- Employees, agents, advisors, freelancers of the data exporter (who are natural persons), and their family members
- The data exporter's Users authorized by the data exporter to use the Services

Categories of personal data transferred

- First and last name
- Title
- Position
- Employer
- Contact information (company, email, phone, physical business address)
- ID data
- Professional life data
- Professional skills information
- Personal life data
- Health and medical information
- Employee compensation information
- Connection data
- Localisation data

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.

The data exporter may submit special categories of data to the SCC Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which is for the sake of clarity Personal Data with information revealing racial or ethnic origin, trade-union membership, and the processing of data concerning health.

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

On a continuous basis throughout the term of the Agreement.

Nature of the processing

Storage, back-up, recovery and processing of Customer Data in connection with a Technical Support case.

Purpose(s) of the data transfer and further processing

As necessary to perform the Services pursuant to the Agreement, as further specified in the Documentation, and as further instructed by Customer in its use of the Services

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 duration of the Agreement.

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

Storage, back-up, recovery and processing of Customer Data in connection with a Technical Support case.

C. **COMPETENT SUPERVISORY AUTHORITY**

Identify the competent supervisory authority/ies in accordance with **clause** 13

The Data exporter's competent supervisory authority will be determined in accordance with the GDPR.

Annex 2

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

EXPLANATORY NOTE:

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

Description of the technical and 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.

The Data importer will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data uploaded to the SCC Services, as described FinancialForce Security, Privacy and Architecture Documentation applicable to the specific SCC Services purchased by data exporter or otherwise made reasonably available by data importer. Data importer will not materially decrease the overall security of the SCC Services during a subscription term.

Attachment 3

Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date	The date of signature of the DPA	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: Trading name (if different): Main address (if a company registered address): Official registration number (if any) (company number or similar identifier):	Full legal name: FinancialForce.com, Inc. Main address (if a company registered address): As indicated in Annex 1 of the DPA
Key Contact	Full Name (optional): Job Title: Contact details including email:	Job Title: Privacy Officer Contact details including email: privacy@financialforce.com

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☐ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: Reference (if any): Other identifier (if any):

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: As indicated in Annex 1 of the DPA
Annex 1B: Description of Transfer: As indicated in Annex 1 of the DPA
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: As indicated in Annex 2 of the DPA
Annex III: List of Sub processors (Modules 2 and 3 only): See section 5 of the DPA

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: x Importer x Exporter

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.

Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

    a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

    b. In Clause 2, delete the words:

        "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";

    c. Clause 6 (Description of the transfer(s)) is replaced with:

        "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

    d. Clause 8.7(i) of Module 1 is replaced with:

        "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

    e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

        "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f. References to "Regulation (EU) 2016/679", "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)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

> "the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

> "These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

> "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

    a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
    b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

a its direct costs of performing its obligations under the Addendum; and/or

b its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.