Data Processing Addendum – November 08, 2024

This Data Processing Addendum (this "DPA") forms a part of the 2Ring Cloud Agreement, as updated or amended from time to time the "Agreement"), between you, the Subscriber and 2Ring. All capitalized terms not defined in this DPA have the meaning set out in the Agreement. In the event of a conflict between the terms and conditions of this DPA and the Agreement, the terms and conditions ofthis DPA shall supersede and control but solely with respect to the subject matter hereof.

This DPA only applies if and to the extent 2Ring Processes Personal Data on behalf of a Subscriber that qualifies as a Data Controller with respect to Personal Data under Applicable Data Protection Law (as defined below). If the Subscriber had entered into earlier data processing terms with 2Ring, those terms are replaced by this DPA.

1. Definitions.

1.1. "**Applicable Data Protection Laws**" means all data protection and privacy laws applicable to the respective party in its role in the Processing of Personal Data under the Agreement, including, where applicable, (i) the EU & UK Data Protection Law and the Swiss FADP, (ii) PIPEDA and any applicable provincial law declared substantially similar to PIPEDA, and (iii) laws of the United States, including the CCPA, the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Utah Consumer Privacy Act, and the Connecticut Act Concerning Personal Data Privacy and Online Monitoring.

1.2. "**California Consumer Privacy Act**" or "**CCPA**" means the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020, and as may be further amended from time to time.

1.3. "**Data Controller**" or "**Controller**" means an entity that determines the purposes and means of the Processing of Personal Data and includes similarly defined terms in Applicable Data Protection Laws, including "business" as that term is defined under the CCPA.

1.4. "**Data Processor**" or "**Processor**" means an entity that Processes Personal Data on behalf of a Data Controller and includes similarly defined terms in Applicable Data Protection Laws, including "service provider" as that term is defined under the CCPA.

1.5. "**Data Subject**" means an identified or identifiable natural person to whom Personal Data relates.

1.6. "**EEA**" means the European Economic Area.

1.7. "**EU & UK Data Protection Law**" means (i) Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 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 or "**EU GDPR**"); (ii) the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (as amended) (the "**UK GDPR**"); (iii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; and (iv) any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (i), (ii) or (iii); (in each case, as may be amended, superseded or replaced from time to time).

1.8. "**PIPEDA**" means the Canadian Personal Information Protection and Electronic Documents Act, 2000.

1.9. "**Restricted Transfer**" means: (i) where the EU GDPR applies, a transfer of EU Personal Data from the European Economic Area to a country outside of the European Economic Area which is not subject to an adequacy determination by the European Commission; (ii) where the UK GDPR applies, a transfer of UK Personal Data from the United Kingdom to any other country which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and (iii) where the Swiss FADP applies, a transfer of Swiss Personal Data from Switzerland to any other country which is not determined to provide adequate protection for Personal Data by the Federal Data Protection and Information Commission or Federal Council (as applicable).

1.10. "**Services**" means the 2Ring Service and any other services related thereto, including hosting and storage, backup and disaster recovery, patches, updates and upgrades, monitoring and testing, data and system security, maintenance, and support and technical services, provided by 2Ring and its Affiliates to Subscriber and its Users under the Agreement and Additional Policies.

1.11. "**Personal Data**" or "**Personal Information**" has the meaning given to such term in Applicable Data Protection Laws including the definition of "personal information" in the CCPA.

1.12. "**Processing**" and its variants namely, "**Process**", "**Processes**" and "**Processed**", shall mean any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission or dissemination, and includes similarly defined terms in Applicable Data Protection Laws.

1.13. "**Purposes**" shall mean (a) 2Ring's or its Affiliate's provision of the Services, (b) the documented, reasonable instructions from Subscriber, or (c) any other purposes agreed in writing by the parties.

1.14. "**Security Incident**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Personal Data.

1.15. "**Standard Contractual Clauses**" **or "SCCs"** means:

(a) In respect of EU Personal Data, the Standard Contractual Clauses for Processors as approved by the European Commission in the form set out in Exhibit 1 of this DPA, with respect to Personal Data that is transferred to a country outside the EEA not recognized as providing an adequate level of protection for Personal Data as described in the EU GDPR (the "**EU Standard Contractual Clauses**" or "**EU SCCs**");

(b) In respect of Swiss Personal Data, the EU Standard Contractual Clauses, provided that any references in the clauses to the GDPR shall refer to the FADP; the term 'member state' must not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence in accordance with clause 18(c) of the EU Standard Contractual Clauses; and

(c) In respect of UK Personal Data, the International Data Transfer Addendum to the EU Standard Contractual Clauses, issued by the Information Commissioner and laid before Parliament in accordance with s.119A of the Data Protection Act 2018 on 2 February 2022 but as permitted by Section 17 of such International Data Transfer Addendum, with the format of the information set out in Part 1 of the Addendum amended as set out in Section 11.1.c, all in the form set out in Exhibit 2 of this DPA **("UK Addendum").**

1.16. "**Subprocessor**" means any other Data Processors engaged by 2Ring to Process Personal Data.

1.17. "**Swiss FADP**" means the Swiss Federal Act on Data Protection 1992 (including as amended or superseded).

1.18. "**Swiss Personal Data**" means Personal Data that is subject to the Swiss FADP.

1.19. "**UK Personal Data**" means Personal Data that is subject to the UK GDPR.

2. Scope and Applicability of this DPA. This DPA applies where and only to the extent that 2Ring Processes Personal Data on behalf of Subscriber as Data Processor in the course of providing the Services. This DPA supplements the 2Ring Privacy Policy available at https://www.2Ring.com/Privacy.

3. Roles and Scope of Processing

3.1. Role of the Parties. As between 2Ring and Subscriber, Subscriber is the Data Controller of Personal Data, and 2Ring will Process Personal Data only as a Data Processor acting on behalf of Subscriber and, with respect to CCPA, as a "service provider" as defined therein.

3.2. Subscriber Instructions. 2Ring will Process Personal Data only for the Purposes. Subscriber shall ensure its Processing instructions are lawful and that the Processing of Personal Data in accordance with such instructions will not violate Applicable Data Protection Laws. The parties agree that the Agreement (including this DPA) sets out Subscriber's complete and final instructions to 2Ring for the Processing of Personal Data. Any Processing outside the scope of these instructions will require prior written agreement between Subscriber and 2Ring.

3.3. Subscriber Affiliates. 2Ring's obligations set forth in this DPA shall also extend to Affiliates of Subscriber, subject to the following conditions:

(a) Subscriber must communicate any additional Processing instructions from its Affiliates directly to 2Ring;

(b) Subscriber shall be responsible for its Affiliates' compliance with this DPA and all acts and/or omissions by its Affiliate with respect to Subscriber's obligations in this DPA shall be considered the acts and/or omissions of Subscriber; and

(c) Subscriber agrees that Subscriber's Affiliates may not bring a claim directly against 2Ring. If an Affiliate of Subscriber seeks to assert a legal demand, action, suit, claim, proceeding or otherwise against 2Ring or its Affiliates: (i) Subscriber must bring Subscriber's Affiliate's claim directly against 2Ring on behalf of such Affiliate, unless Applicable Data Protection Laws require the Affiliate be a party to such claim; and (ii) all Subscriber Affiliate claims shall be considered claims made by Subscriber and shall be subject to any liability restrictions set forth in the Agreement, including any aggregate limitation of liability.

3.4. Subscriber Processing of Personal Data. Subscriber agrees that it: (a) will comply with its obligations under Applicable Data Protection Laws with respect to its Processing of Personal Data; (b) will make appropriate use of the 2Ring Service to ensure a level of security appropriate to the particular content of the Personal Data; and (c) has obtained all consents, permissions and rights necessary under Applicable Data Protection Laws for 2Ring to lawfully Process Personal Data for the Purposes, including Subscriber's sharing and/or receiving of Personal Data with third-parties via Subscriber's the use of the Services.

3.5. Details of Data Processing

(a) Subject matter: The subject matter of the Processing under this DPA is the Personal Data.

(b) Duration: Notwithstanding expiry or termination of the Agreement, this DPA and Standard Contractual Clauses (if applicable) will remain in effect until, and will automatically expire upon, deletion of all Personal Data as described in this DPA.

(c) Purpose: 2Ring will Process Personal Data only for the Purposes.

(d) Nature of the Processing: 2Ring provides Services as described in the Agreement.

(e) Categories of Data Subjects: The categories of Data Subjects to which Personal Data relate are determined and controlled by Subscriber in its sole discretion, and may include, but are not limited to:

(i) Employees, agents, or contractors of Subscriber, who are natural persons.

(ii) Employees, agents, or contractors of Subscriber's Affiliates, who are natural persons.

(iii) Employees, agents or contractors of Subscriber's or its Affiliate's contractors, who are natural persons.

(iv) Any other individuals authorized to use the 2Ring Service by Subscriber or its Affiliates pursuant to the Agreement and the DPA.

(f) Types of Personal Data: The types of Personal Data Processed by the Services are determined and controlled by Subscriber in its sole discretion, and may include, but are not limited to:

(i) Identification and contact data (name, email, and login identifier);

(ii) Employment details (employee name, phone extension, role and work assignment); and/or

(iii) IT information (IP address, browser type and version, language, usage data, and cookies data).

(g) Special Categories of Personal Data (if applicable): Unless explicitly agreed in writing by 2Ring and Subscriber, the Subscriber will not disclose (and will not permit any Data Subject to disclose) any special categories of

Personal Data to 2Ring for Processing.

4. Subprocessing

4.1. **Subprocessors**. Subscriber generally authorizes the engagement of Subprocessors and specifically consents to those listed on 2Ring's subprocessor list at https://www.2ring.com/LegalCloud ("**Subprocessor List**").

4.2. **Subprocessor Obligations**. 2Ring will: (a) impose data protection obligations on Subprocessors it appoints to Process Personal Data in accordance with Applicable Data Protection Law, taking into account the nature of the services provided by such Subprocessor; and (b) remain liable for each Subprocessor's compliance with the obligations in this DPA. Upon written request, 2Ring will provide Subscriber all relevant information Subscriber reasonably requests in connection with its applicable Subprocessor agreements where required to satisfy Subscriber's obligations under Applicable Data Protection Laws.

4.3. **Changes to Subprocessors.** 2Ring will make available on www.2Ring.com/LegalCloud a mechanism for Subscriber to subscribe tonotifications of updates to the Subprocessor List. 2Ring will not allow a new Subprocessor to Process Personal Data without posting the name of the new Subprocessor on the Subprocessor List for at least fourteen (14) days. The Subscriber may object to 2Ring's appointment or replacement of a Subprocessor during such fourteen (14) day period, provided such objection is based on reasonable grounds relating to data protection. In such event, the parties will discuss Subscriber's concerns in good faith with a view toachieving resolution. If Subscriber can reasonably demonstrate that the new Subprocessor is unable to Process Personal Data in compliance with the terms of this DPA and 2Ring determines, in its sole discretion, that it is not commercially reasonable to provide an alternative Subprocessor, or the parties are not otherwise able to achieve resolution as provided in the preceding sentence, Subscriber, as its sole and exclusive remedy, may cease using the 2Ring Service.

5. Security

5.1. **Security Measures**. 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, 2Ring will maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk of Processing the Personal Data described in Section 3.5(f) above.

5.2. **Confidentiality of Processing**. Any person who is authorized by 2Ring or its Affiliate to Process Personal Data (including each of their respective employees, agents and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

5.3. **No Assessment of Personal Data by 2Ring**. 2Ring will have no obligation to assess the contents of Personal Data to identify information subject to any specific legal requirements. Subscriber is responsible for reviewing the information made available by 2Ring relating to data security and making an independent determination as to whether theServices meet Subscriber's requirements and legal obligations under Applicable Data Protection Laws.

6. Subscriber Audit Rights

6.1. Upon written request and at no additional cost to Subscriber, 2Ring will provide Subscriber, or its appropriately qualified third-party representative (collectively, the "**Auditor**"), access to reasonably requested documentation evidencing 2Ring's compliance with its obligations under this DPA in the form of its current ISO/IEC 27001:2013 Certification.

6.2. Subscriber may also send a written request for an audit (including inspection) of 2Ring's facilities. Following receipt by 2Ring of such request, 2Ring and Subscriber shall mutually agree in advance on the details of the audit, including reasonable start date, scope and duration of, and security and confidentiality controls applicable to, any such audit. 2Ring may charge a fee(rates shall be reasonable, taking into account the resources expended by 2Ring) for any such audit. The reports, audit, and any information arising therefrom shall be 2Ring's Confidential Information.

6.3. Where the Auditor is a third-party, the Auditor may be required to execute a separate confidentiality agreement with 2Ring prior to any review of reports or an audit of 2Ring, and 2Ring may object in writing to such Auditor, if in 2Ring's reasonableopinion, the Auditor is not suitably qualified or is a direct competitor of 2Ring. Any such objection by 2Ring will require Subscriber to either appoint another Auditor or conduct the audit itself. Expenses incurred by Auditor in connection with any review of Reports or an audit, shall be borne exclusively by Subscriber or the Auditor.

For clarity, the exercise of audit rights under the Standard Contractual Clauses shall be as described in this Section 6 (Subscriber Audit Rights).

7. Data Transfers

7.1. Hosting and Processing Locations. A list of available of geographic regions to choose from for the hosting of the Subscription is available at https://www.2Ring.com/HostingRegions (the "**Available Hosting Regions List**"). 2Ring may offer hosting in new regions in the future by amending the Available Hosting Regions List. Either the applicable Order will specify, and if not, then during 2Ring's onboarding process for the Subscriber, Subscriber may specify, the geographic region from the Available Hosting Regions List, in which Subscriber's Subscription and all related Personal Data will be hosted (the "**Hosting Region**"). Subscriber is solely responsible for the regions from which its Users upload or access the Personal Data, for any transfer or sharing of Personal Data by Subscriber or its Users. 2Ring will not Process Personal Data from outside the Hosting Region except as reasonably necessary to provide the Services procured by Subscriber, or as necessary to comply with applicable law or binding order of a governmental body.

7.2. Certain Transfer Mechanisms. With respect to Restricted Transfers by Subscriber of Personal Data to 2Ring in a country other than a country which ensures an adequate level of protection, within the meaning of and to the extent governed by the Applicable Data Protection Laws of the such country (each country that provides such adequate level of protection, an "**Adequate Country**"), such transfers shall be governed by the appropriate Standard Contractual Clauses as provided in Sections 7.2.1, 7.2.2 and 7.2.3, as applicable, which are incorporated into this DPA. For these purposes 2Ring will be the "data importer" and Subscriber is the "data exporter" under the applicable Standard Contractual Clauses (notwithstanding that Subscriber may be an entity located outside of an Adequate Country). You also authorize 2Ring to enter into the applicable Standard Contractual Clauses as your agent and on your behalf with any Subprocessor of Personal Data who is not located in an Adequate Country where this is necessary for compliance with Applicable Data Protection Law.

7.2.1 In relation to Restricted Transfers of EU Personal Data, Module Two of the EU Standard Contractual Clauses set forth in Exhibit 1 to this DPA applies.

7.2.2 In relation to Restricted Transfers of UK Personal Data, the UK Addendum set forth in Exhibit 2 of this DPA applies and each party shall be deemed to have signed the UK Addendum.

7.2.3 In relation to Restricted Transfers of Swiss Personal Data, the EU Standard Contractual Clauses shall apply amended as follows:

(i) references to "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss FADP;

(ii) references to specific Articles of "Regulation (EU) 2016/679" shall be replaced with the equivalent article or section of the Swiss FADP;

(iii) references to Regulation (EU) 2018/1725 shall be removed;

(iv) references to "EU", "Union" and "Member State" shall be replaced with references to "Switzerland";

(v) Clause 13(a) is not used and for purposes of Part C of Annex I, the "competent supervisory authority" shall be the Swiss Federal Data Protection Information Commissioner;

(vi) references to the "competent supervisory authority" and "competent courts" shall be replaced with references to the "Swiss Federal Data Protection Information Commissioner" and "applicable courts of Switzerland" ;

(vii) in Clause 17, the EU Standard Contractual Clauses shall be governed by the laws of Switzerland; and

(viii) Clause 18 shall be replaced to state: "Any dispute arising from these Clauses shall be resolved by the competent courts of Switzerland. The Parties agree to submit themselves to the jurisdiction of such courts".

8. Return or Deletion of Data. 2Ring will retain Personal Data for a period of not more than thirty (30) days after a

Subscription is terminated, unless 2Ring has any other legitimate business purpose or legal requirement for longer retention of Personal Data. On expiry of this period or on the Subscriber's earlier request, 2Ring will delete or return Personal Data in our possession or control in a manner and form decided by 2Ring, acting reasonably. This requirement will not apply to the extent that 2Ring is required by applicable law to retain some or all Personal Data, or to Personal Data it has archived on back-up systems, which Personal Data 2Ring will securely isolate and protect from any further processing.

9. Security Incident Response

9.1. Security Incident Reporting. If 2Ring becomes aware of a Security Incident, 2Ring will notify Subscriber without undue delay, and in any case, where feasible, within forty-eight (48) hours after becoming aware. 2Ring will promptly take reasonable steps to contain, investigate, and mitigate any Security Incident.

9.2. Security Incident Communications. 2Ring will provide Subscriber information about the Security Incident, including the nature and consequences of the Security Incident, the measures taken and/or proposed by 2Ring to mitigate or contain the Security Incident, the status of 2Ring's investigation, a contact point from which additional information may be obtained, and the categories and approximate number of data records concerned. Communications by or on behalf of 2Ring with Subscriber in connection with a Security Incident shall not be construed as an acknowledgment by 2Ring of any fault or liability with respect to the Security Incident.

10. Cooperation

10.1. Data Subject Requests. To the extent legally permitted, 2Ring will promptly notify Subscriber if 2Ring receives a request from a Data Subject that identifies Subscriber and seeks to exercise the Data Subject's right to access, rectify, erase, transfer or port Personal Data, or to restrict the Processing of Personal Data (each, a "**Data Subject Request**"). Subscriber will be responsible for responding to any such Data Subject Request. To the extent Subscriber is unable to access the relevant Personal Data within the 2Ring Service taking into account the nature of the Processing, 2Ring will, upon Subscriber's written request and at Subscriber's expense, provide commercially reasonable cooperation to assist Subscriber in responding to any Data Subject Requests.

10.2. Data Protection Impact Assessments. 2Ring will provide reasonably requested information regarding the Services to enable Subscriber to carry out data protection impact assessments or prior consultations with data protection authorities as required by Applicable Data Protection Laws, so long as Subscriber does not otherwise have access to the relevant information.

10.3. Government, Law Enforcement, and/or Third Party Inquiries. If 2Ring receives a demand from any third party, including law enforcement or a governmental authority (each, a "**Third-Party Demand**"), to retain, disclose, or otherwise Process Personal Data then 2Ring will attempt to redirect the Third-Party Demand to Subscriber. Subscriber agrees that 2Ring can provide information to such third party as reasonably necessary to redirect the Third-Party Demand. If 2Ring cannot redirect the Third-Party Demand to Subscriber, then 2Ring will, to the extent legally permitted to do so, provide Subscriber notice of the Third-Party Demand reasonably promptly under the circumstances to allow Subscriber to seek a protective order or other appropriate remedy.

11. Changes in Applicable Data Protection Laws. Subscriber may by written notice propose variations to this DPA or the applicable Standard Contractual Clauses which are required as a result of any change in, or decision of a competent authority under any Applicable Data Protection Law, or propose any other changes to this DPA which Subscriber reasonably considers necessary to address the requirements of Applicable Data Protection Law. Except to the extent required by Applicable Data Protection Law, any such change or variation shall not be binding on 2Ring unless accepted in writing by an authorized representative of 2Ring. 2Ring may, upon written notice to Subscriber sent within thirty (30) days' of the receipt of Subscriber's notice, cease providing the affected 2Ring Services or terminate any affected Order or the Agreement without liability if 2Ring believes it will not be commercially practicable or otherwise be reasonably able to comply with such proposed variations or changes.

12. Relationship with the Agreement

12.1. Except as provided by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict in connection with the Processing of Personal Data.

12.2. Notwithstanding anything to the contrary in the Agreement or this DPA, each party's and all of its Affiliates' liability, takentogether in the aggregate, arising out of or relating to this DPA, the Standard Contractual Clauses, and any other data protection agreements in connection with the Agreement (if any), shall be subject to any aggregate limitations on liability set out in the Agreement.

12.3. In no event shall this DPA, the Agreement, or any party to the Agreement, restrict or limit the rights of any Data Subject or of any competent supervisory authority.

12.4. This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement.

Exhibit 1 to the DPA: EU STANDARD CONTRACTUAL CLAUSES

STANDARD CONTRACTUAL CLAUSES

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)[1] for the transfer of personal 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.

---

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision […].

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 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(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.

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.

Transfer controller to processor

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 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 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[2] (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.

[2] 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.

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 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) 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 fourteen (14) 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.[3] 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.

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

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

Clause 10

Data subject rights

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

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

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

Clause 11

Redress

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

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

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

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

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

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

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

Clause 12

Liability

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

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

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

of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

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

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

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

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

Clause 13

Supervision

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

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

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

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

(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[4];

(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.

Clause 15

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

[4] 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.

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 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 Member State in which the data exporter is established.

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 Member State in which the data exporter is established.

(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

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]*

1.	Name:	The party identified in the applicable Order as the "Subscriber" for the purposes of the Agreement and this DPA
	Address:	The address provided in the Order
	Contact person's name, position and contact details:	As set out in the Order
	Activities relevant to the data transferred under these Clauses:	See B. below
	Signature and date:	Acceptance of the Agreement as per Agreement
	Role (controller/processor):	Controller

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

1.	Name:	2Ring America, Inc. ("2Ring")
	Address:	3626 Fair Oaks Blvd., Suite 100 Sacramento, CA 95864 USA
	Contact person's name, position and contact details:	Michal Grebac, Strategic Sales & Marketing Director
	Activities relevant to the data transferred under these Clauses:	See B. below
	Signature and date:	Acceptance of the Agreement as per Agreement
	Role (controller/processor):	Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:	Subscriber may submit personal data to the 2Ring Service, the extent of which is determined and controlled by Subscriber in its sole discretion, and which may include, but is not limited to, personal data relating to the categories of data subjects specified in Section 3.5(e) of the DPA.
Categories of personal data transferred:	The categories of personal data processed by 2Ring are determined and controlled by Subscriber in its sole discretion and may include but are not limited to the categories of personal data specified in Section 3.5(f) of the DPA.
Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:	No sensitive data is necessary for the use of the 2Ring Service. However, the types of personal data processed by the 2Ring Service are determined and controlled by Subscriber. Unless explicitly agreed in writing by 2Ring and Subscriber, the Subscriber will not disclose (and will not permit any data subject to disclose) any special categories of personal data to the 2Ring Service or 2Ring.
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):	Continuous

Nature of the processing:	2Ring and its Affiliates will process personal data to provide Subscriber and its Users the 2Ring Service and any other services, including support and technical services, under the Agreement and Additional Policies. personal data transferred will be processed in accordance with the Agreement and may be subject to the following processing activities: (A) storage and other processing necessary to provide, maintain, secure, backup, and improve the 2Ring Service, as applicable, provided to Subscriber; and/or (B) disclosures in accordance with the Agreement and the DPA, and/or as compelled by applicable law.
Purpose(s) of the data transfer and further processing:	Processing (a) to perform any steps necessary for the performance of the Agreement; (b) to provide the Services in accordance with the Agreement; (c) initiated by Users in their use of the 2Ring Service; (d) to comply with other reasonable instructions provided by Subscriber that are consistent with the terms of the Agreement and the DPA; and (e) to comply with any legal obligations under applicable law, including Applicable Data Protection Laws.
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:	The duration of the Agreement plus the period from the expiry of the Agreement until deletion of the personal data in accordance with the DPA.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance (e.g. in accordance with Clause 13 SCCs)	The competent supervisory authority, in accordance with Clause 13 of the EU SCCs, is either (i) the supervisory authority applicable to the data exporter in its EEA country of establishment or, (ii) where the data exporter is not established in the EEA, the supervisory authority applicable in the EEA country where the data exporter's EU representative has been appointed pursuant to Article 27(1) of the EU GDPR, or (iii) where the data exporter is not obliged to appoint a representative, the supervisory authority applicable to the EEA country where the data subjects relevant to the transfer are located. With respect to personal data regulated by the UK GDPR, the competent supervisory authority is the Information Commissioners Office. With respect to the processing of personal data to which the Swiss FADP applies, the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner. With respect to the processing of personal data to which PIPEDA applies, the competent supervisory authority is the Office of the Privacy Commissioner of Canada.

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organizational measures implemented by the processor(s) / 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.

Measure	Description
Measures of pseudonymisation and encryption of personal data	• Personal data is encrypted at rest via disc encryption mechanisms at the disc level
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	• Access controls are implemented to enforce confidentiality, integrity and availability. • Access to in-scope systems requires a user ID plus SSH Keys and/or password authentication. Where passwords are used, password parameters enforce minimum length, password age and complexity requirements. • Privileged access to 2Ring Service systems is restricted to appropriate personnel. • Access to 2Ring Service production systems is logically and physically segregated from the 2Ring network. • Subscriber environments are separated from each other at network level • Subscriber keys used to access source data while importing are encrypted using modern and secure algorithms • Access to personal data via the 2Ring Service supports Multifactor Authentication Mechanisms if Subscriber has a Microsoft Azure AD license and configures Microsoft Azure AD Multifactor Authentication • Access to personal data via the 2Ring Service requires use of strong passwords that must meet the minimum complexity requirements with strong defaults • The 2Ring Service provides mechanism for Subscriber to segregate personal data into smaller parts with access controls to minimize access to these parts to unauthorized personnel of the Subscriber • The 2Ring Service uses industry standard and established external Identity Providers: MS Azure AD, OKTA • Antivirus software is used to protect 2Ring workstations used to access the 2Ring Service system from malicious code or viruses. • 2Ring reviews automated alerts for unauthorized attempts to access production data.
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	• Databases and file repositories containing personal data are backed up at regular intervals throughout the day by an automated process. • Data backups are stored off site from the original environment but within the same Hosting Region. • Backup restorations are tested on at least a quarterly basis. • Backups are configured to be retained for at least seven days. • The 2Ring Service is built in a redundant, self-healing and scalable manner, to automatically recover from local failures. • Disaster recovery plans are in place and tested regularly.

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	• Building blocks of the 2Ring Service are reviewed for security vulnerabilities at regular intervals • Automated vulnerability scans are performed at regular intervals • 2Ring performs yearly audits of its conformance with the ISO/IEC 27001 certification
Measures for user identification and authorisation	• Access to the 2Ring Service operational and production environments is protected by use of unique user accounts, strong passwords, use of Multi-Factor Authentication (MFA), role-based access, and least privilege principle. • Identity and access management processes for 2Ring user account provisioning, de-provisioning and changes are enforced.
Measures for the protection of data during transmission	• All transfer paths of personal data are encrypted within the hosting environment and during import (TLS) • Access to personal data from outside the hosting environment is only available via encrypted transfer mechanisms (HTTPS/TLS)
Measures for the protection of data during storage	• Access controls restrict access to personal data. • Personal data in the 2Ring Service is encrypted. • Personal data is logically segregated on its own database. • Endpoint security software is used to protect 2Ring workstations used to access the 2Ring Service system from malicious code or viruses.
Measures for ensuring physical security of locations at which personal data are processed	• 2Ring utilizes Microsoft Azure for its production environments. The physical and environmental controls related to the facilities housing the production environments are managed by the subservice organization. • The subservice organization SOC reports are reviewed on an annual basis in accordance with 2Ring's security standards.
Measures for ensuring events logging	• The hosting environment is equipped with automatic logging mechanisms of security events. • The 2Ring Service emits logs of its operation and/or failures. • Both types of events logged as described above are reviewed regularly.
Measures for ensuring system configuration, including default configuration	• The 2Ring Service is deployed with meaningful and secure defaults • System configuration is versioned • All changes to configuration of the 2Ring Service are logged • 2Ring Service configuration is backed up to an off-site location
Measures for internal IT and IT security governance and management	• 2Ring has a documented Information Security Management System (ISMS). • 2Ring has a documented Information Security Policy (which is part of the ISMS), which is approved by 2Ring's management team ("2Ring Management"). • 2Ring has a documented Secure Development Life Cycle process (which is a part of the ISMS) that governs development of the 2Ring Service and its operation. • The 2Ring Management provides oversight over the ISMS through periodic updates on risk assessments, third-party attack and penetration studies, and compliance with the Information Security Policy.

	• The ISMS Manager is accountable for the security, availability and confidentiality of information assets and 2Ring Service security. ISMS Manager is supported by the Chief Information Officer. • The 2Ring Management has authorized the ISMS Manager to enforce the ISMS. • A formal security awareness program is in place to make all employees and contractors of 2Ring and its Affiliates aware of 2Ring's security policy, standards, and information security obligations. • Employees are required to read and sign confidentiality agreements, and accept company policies and code of conduct.
Measures for certification/assurance of processes and products	• 2Ring performs yearly audits of its conformance with the ISO/IEC 27001 Information Security standard by an accredited external auditing organization. • 2Ring performs quarterly internal audits of its conformance with the ISO/IEC 27001 Information Security standard.
Measures for ensuring data minimisation	• 2Ring limits data collection to the purposes of processing (or the data that the Subscriber chooses to provide). • Security measures are implemented to provide 2Ring employees with only the minimum amount of access necessary to perform required functions.
Measures for ensuring data quality	• Subscribers have ownership and control over personal data in the 2Ring Service.
Measures for ensuring limited data retention	• Data backups are retained to support 2Ring Service system recovery operations in the event of a disaster or other contingency. 2Ring does not make specific Subscriber commitments for data retention. • Data for Subscription customers is removed after the end of the Subscription Term and upon written notice by the Customer.
Measures for ensuring accountability	• The ISMS defines roles and their respective accountability and responsibility within 2Ring • 2Ring's ISMS, Employee Handbook and employee contracts contain employee sanctions on noncompliance with policies. • 2Ring policies require violations of the Information Security Policy or Employee Handbook to be reported to 2Ring's or its Affiliate's HR and/or Security Council. • 2Ring has agreements with its subcontractors that includes requirements to comply with applicable laws and protect the confidentiality of data.
Measures for allowing data portability and ensuring erasure	• Subscribers have ownership and control over their personal data in the 2Ring Service.

ANNEX III – LIST OF SUB-PROCESSORS

EXPLANATORY NOTE:

In accordance with Clause 9(a) Option 2, the controller has authorised the use of the sub-processors from the list that can be found here: https://www.2ring.com/LegalCloud

Information Commissioner's Office

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	Start date is the date Subscriber accepts the 2Ring Cloud Agreement available at https://www.2ring.com/CloudAgreement (the "Agreement") in accordance with the Agreement. All capitalized terms not defined herein have the meaning set out in the Agreement or the Data Processing Addendum that forms a part of the Agreement (the "DPA").	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: Subscriber as named in the applicable Order under the Agreement Trading name (if different): As set out in the applicable Order Main address (if a company registered address): As set out in the applicable Order Official registration number (if any) (company number or similar identifier): If any, as set out in the applicable Order	Full legal name: The applicable 2Ring entity's full legal name as set out in, and in accordance with, the Agreement Trading name (if different): Main address (if a company registered address): As set out in the Agreement Official registration number (if any) (company number or similar identifier): If any, as set out in the Agreement

Key Contact	Full Name (optional): Job Title: Contact details including email:	Full Name (optional): Job Title: Contact details including email:
Signature (if required for the purposes of Section 2)		

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☒ The version of the Approved EU SCCs set forth in Exhibit 1 to the DPA, and to which DPA this Addendum is appended to, detailed below, including the Appendix Information: Date: June 4, 2021 Reference (if any): The version set forth in Exhibit 1 to the DPA before this Addendum. Other identifier (if any): Or ☐ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1						
2						
3						
4						

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 listed in Annex 1 to the EU SCCs included in Exhibit 1 to the DPA.

Annex 1B: Description of Transfer: As listed in Annex 1 to the EU SCCs included in Exhibit 1 to the DPA.

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: As listed in Annex II to the EU SCCs included in Exhibit 1 to the DPA.

Annex III: List of Sub processors (Modules 2 and 3 only): As listed in Annex 3 to the EU SCCs included in Exhibit 1 to 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: ☒ Importer ☒ Exporter ☐ neither Party

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.

Alternative Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 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 of those Mandatory Clauses.