Data Processing Addendum

This Data Processing Addendum ("**DPA**") is made as of the Effective Date and applies where and only to the extent that Personal Data protected under Data Protection Laws are processed by R3 HoldCo LLC and/or its subsidiaries (jointly referred to as "**R3**") in the context of their activities and/or services (jointly referred to as "**R3 Services**").

The scope of the R3 Services and corresponding processing of Personal Data is determined by the scope of the agreement entered into by and between R3 and a Counterparty, as defined below (the "**Agreement**"). This DPA is incorporated by reference in, and forms part of, each Agreement.

R3 and Counterparty are also referred to herein individually as a "**Party**" and collectively as the "**Parties**."

1. Definitions

"**Agreement**" means the agreement relating to R3 Services entered into by and between R3 and Counterparty.

"**Authorized Party**" means a party, if any, other than Counterparty that is duly authorized to use R3 Services under the Agreement.

"**B2B Personal Data**" means Personal Data exchanged between and processed by the Parties for entering into legal agreements, for billing and invoicing purposes, or for any other business-to-business communications, including but not limited to Personal Data of representatives, employees or contractors of the Parties.

"**Counterparty**" means the party that has entered into an Agreement. By means of example and not limitation, a "Counterparty" can be the Customer in a Master License and Professional Services agreement, or the Participant in a Sponsoring Participant Terms of Use agreement.

"**Counterparty Personal Data**" means Personal Data other than B2B Personal Data provided by Counterparty or an Authorized Party (as applicable) that R3 processes on its or their behalf.

"**Data Protection Laws**" means all data protection and privacy laws applicable to the processing of Personal Data under the Agreement, including, where applicable, EU Data Protection Law.

"**DPA**" means this Data Processing Addendum, that forms part of an Agreement.

"**EEA**" means, for the purposes of this DPA, the European Economic Area and/or their member states and/or Switzerland.

"**Effective Date**" means the date of execution of the Agreement.

"**EU Data Protection Law**" means Regulation 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 or "**GDPR**") and applicable national implementations of the GDPR, as well as, for the sole purpose of this DPA, the UK GDPR and the UK Data Protection Act 2018; each as may be amended, superseded or replaced.

"**GDPR**" means Regulation 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).

"**Party**" means R3 or Counterparty.

"**Parties**" means R3 and Counterparty.

"**Personal Data**" means any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular natural person or household, as defined in applicable Data Protection Laws.

"**R3**" means R3 HoldCo LLC and/or its subsidiaries.

"**R3 Services**" means activities and/or services of R3.

"**Standard Contractual Clauses**" means the standard contractual clauses adopted by the European Commission for the transfer of Personal Data to processors established in Third Countries..

"**SCCs 2010**" means the Standard Contractual Clauses adopted by the European Commission by means of Commision Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (OJ L 39, 12.2.2010, p. 5).

"**SSCs 2021**" means the Standard Contractual Clauses adopted by the European Commission by means of Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (OJ L 199, 7.6.2021, p. 31)."**Security Incident**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Counterparty Personal Dta transmitted, stored or otherwise processed.

"**Security Measures**" means the technical and organizational measures taken by R3, as described in Annex II to the SCCs 2021, attached hereto as Exhibit A.

"**Sensitive Data**" means (a) social security number, passport number, driver's license number, or similar identifier (or any portion thereof); (b) credit or debit card number (other than the truncated (last four digits) of a credit or debit card); (c) employment, financial, genetic, biometric or health information; (d) racial, ethnic, political or religious affiliation, trade union membership, or

information about sexual life or sexual orientation; (e) account passwords; or (f) other information that falls within the definition of "special categories of personal data" under the EU Data Protection Law.

"**Third Country**" means any country, territory or specified sector within that country or territory outside of the EEA that is not recognized by the European Commission or any competent authority (including a supervisory authority) as ensuring an adequate level of protection.

"**UK GDPR**" means the GDPR as tailored to the UK regime and applicable in the United Kingdom.

The terms "processing", "controller", "processor", and "data subject" shall have the meaning given to them in the GDPR, and "process", "processes" and "processed" shall be interpreted accordingly.

2. Roles and Responsibilities

2.1. Parties' role. The Parties act as independent controllers when exchanging or otherwise processing B2B Personal Data.

2.2. R3's role. Any processing by R3 of Counterparty Personal Data is carried out as a processor on behalf of Counterparty or Authorized Party (as applicable) solely for purposes of performing R3's obligations under the Agreement. R3 will not retain, use or disclose Counterparty Personal Data for any purpose other than those identified in the Agreement and R3 will only process Counterparty Personal Data in accordance with Counterparty's or Authorized Party's (as applicable) documented lawful instructions, except where otherwise required by applicable law; in such case, R3 shall inform Counterparty of that legal requirement before processing, unless applicable law prohibits such information on important grounds of public interest. For the avoidance of doubt, as Counterparty and Authorized Party (as applicable) make an informed decision to use R3 Services, they determine the purposes and the means of any processing of Counterparty Personal Data on their behalf. In that sense, the Parties agree, and Counterparty shall procure that Authorized Party (as applicable) agrees before providing any Counterparty Personal Data, that the Agreement sets out Counterparty's or Authorized Party's (as applicable) complete and final instructions to R3 in relation to the processing of Counterparty Personal Data. Any processing of Counterparty Personal Data differing from these instructions (if any) shall require prior written agreement between the Parties. R3 shall promptly notify Counterparty if it becomes aware or believes that any data processing instruction from Counterparty or Authorized Party (as applicable) violates Data Protection Laws.

2.3. Counterparty's and Authorized Party's role. By deciding to use R3 Services, Counterparty and Authorized Party (as applicable) determine the purposes and the means of the processing of Counterparty Personal Data.

2.4. Purpose limitation. R3 shall process Counterparty Personal Data only for the purpose described in this DPA and in accordance with the Counterparty's documented lawful instructions, except where otherwise required by applicable law. The parties agree that the Agreement sets out Counterparty's complete and final instructions to R3 in relation to the

processing of Countparty Personal Data, and processing differing from these instrcutions (if any) shall require prior written agreement between the parties.

2.5. Prohibited data. Counterparty will not provide (or cause to be provided) any Sensitive Data to R3 for processing under the Agreement, and R3 will have no liability to Counterparty or any other person whatsoever for Sensitive Data, whether in connection with a Security Incident or otherwise. For the avoidance of doubt, no Sensitive Data will be processed under this DPA.

2.6. Compliance with Data Protection Laws. R3, Counterparty and Authorized Party (as applicable) shall comply with Data Protection Laws in respect of their respective processing of Counterparty Personal Data in such a way as to not expose each other, directly or indirectly, to any violation of Data Protection Laws. If R3, Counterparty or Authorized Party (as applicable) determines that it cannot comply with its obligations under Data Protection Laws, it shall immediately inform the impacted party of that reason, impact and other expected consequences thereof. For the avoidance of doubt, non-compliance with Data Protection Laws shall be considered as a violation of the terms of the Agreement.

3. Information to Data Subjects

3.1. B2B Personal Data. Each Party is responsible for providing the information that is required by Data Protection Laws to individuals whose Personal Data are provided to the other Party as B2B Personal Data.

3.2. Counterparty Personal Data. As R3 does not have any contact or relationship with the individuals whose Personal Data are processed as Counterparty Personal Data, Counterparty and Authorized Party (as applicable) are solely responsible for providing such individuals with the information required by Data Protection Laws.

4. Data Subject Rights and Cooperation

4.1. B2B Personal Data. Each Party is responsible for addressing data subject requests related to B2B Personal Data.

4.2. Cooperation. R3 shall, at Counterparty's expense, provide reasonable cooperation to assist Counterparty or Authorized Party (as applicable) to respond to any requests from individuals or competent supervisory authorities relating to the processing of Counterparty Personal Data by R3 under the Agreement. In the event that such request is made to R3 directly, R3 shall not respond to such communication directly except as appropriate (for example, to direct the data subject to contact Counterparty) or legally required. If R3 is required to respond to such a request, R3 shall promptly notify Counterparty and provide Counterparty with a copy of the request unless R3 is legally prohibited from doing so. For the avoidance of doubt, nothing in an Agreement (including this DPA) shall restrict or prevent R3 from responding to any request from an individual or competent supervisory authority in relation to B2B Personal Data or any other Personal Data for which R3 is a controller.

4.3. Subpoenas and court orders. If a law enforcement agency sends R3 a demand for

Counterparty Personal Data (for example, through a subpoena or court order), R3 shall attempt to redirect the law enforcement agency to request such data directly from Counterparty and Authorized Party (as applicable). As part of this effort, R3 may provide Counterparty's basic contact information. If compelled to disclose Counterparty Personal Data to a law enforcement agency, R3 shall give Counterparty reasonable notice of the demand to allow the latter to seek a protective order or other appropriate remedy, unless R3 is legally prohibited from doing so.

4.4. Data protection impact assessment. To the extent required under applicable Data Protection Laws, R3 shall, at Counterparty's expense, provide all reasonably requested information regarding the processing of Counterparty Personal Data by R3 under the Agreement to enable Counterparty or Authorized Party (as applicable) to carry out data protection impact assessments or prior consultations with supervisory authorities as required by Data Protection Laws.

5. Engaging Other Processors

5.1. Authorization of other processors. Counterparty agrees, and Counterparty shall procure that Authorized Party (as applicable) agrees before providing any Counterparty Personal Data, that R3 may engage sub-processors to process Counterparty Personal Data. The list of sub-processors currently engaged by R3 and authorized by Counterparty and Authorized Party (as applicable) can be accessed here [https://www.r3.com/Sub-Processors-List].

5.2. Objection to other processors. Counterparty and Authorized Party (as applicable) are deemed to be informed of any intended changes concerning the addition or replacement of other processors once these are added to the list referred to in Section 5.1 of this DPA. In case Counterparty or Authorized Party (as applicable) want to be informed via email, they shall inform R3 in writing about this and provide an email address to send the information to. Counterparty or Authorized Party (as applicable) may object in writing to R3's appointment of another processor within seven (7) calendar days after that such processor has been added to the list referred to in Section 5.1 above, provided that such objection is based on reasonable grounds relating to Data Protection Laws. In such event, R3 will take such objection into account in appointing such other processor.

5.3. Other processors' obligations. R3 shall: (i) enter into a written agreement with each other processor containing data protection obligations that provide at least the same level of protection for Counterparty Personal Data as those in this DPA, to the extent applicable to the nature of the services provided by such other processor; and (ii) remain responsible for such other processor's compliance with the obligations of this DPA and for any acts or omissions of such other processor that cause R3 to breach any of its obligations under this DPA.

6. Security

6.1. Security Measures. R3 shall implement and maintain the technical and organizational Security Measures described in Annex II to the SCCs 2021, attached hereto as Exhibit A.

Counterparty and Authorized Party (as applicable) shall be responsible for reviewing the information made available by R3 relating to such Security Measures and for making an independent determination as to whether such measures meet Counterparty's and Authorized Party's (as applicable) requirements and legal obligations under Data Protection Laws.

6.2. Confidentiality. R3 shall ensure that persons authorized to process Counterparty Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

6.3. Updates to Security Measures. Counterparty acknowledges, and Counterparty shall procure that Authorized Party (as applicable) acknowledges before providing any Counterparty Personal Data, that the Security Measures are subject to technical progress and development and that R3 may update or modify them from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the R3 Services.

6.4. Security Incident response. Upon becoming aware of a Security Incident affecting Counterparty Personal Data, R3 shall: (i) notify Counterparty without undue delay; (ii) provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by Counterparty; and (iii) promptly take reasonable steps to contain and investigate any Security Incident. R3's notification of or response to a Security Incident under this Section 6.4 shall not be construed as an acknowledgment by R3 of any fault or liability with respect to the Security Incident.

7. Demonstrating Compliance

7.1. Records. Upon reasonable written request from Counterparty, R3 shall make available to Counterparty all information reasonably necessary to demonstrate compliance with this DPA.

7.2. Audits. Where the GDPR or UK GDPR applies, R3 will allow for and contribute to audits, including inspections, conducted by Counterparty or another auditor mandated by Counterparty.

8. International Transfers

8.1. Data center locations. In the event that R3 transfers and processes Counterparty Personal Data to and in the United States and anywhere else in the world where R3, its subsidiaries or the other processors maintain data processing operations, R3 shall at all times require that such transfers are made in compliance with the requirements of Data Protection Laws.

8.2. EEA Data transfers. By entering into the Agreement, the Parties enter into the SCCs 2021, which are attached as Exhibit A and form and integral part of this DPA, in order to provide appropriate safeguards with regard to Counterparty Personal Data in case of transfers outside of the EEA to a Third Country. For the purposes of the Standard Contractual Clauses, R3 agrees that it is the "data importer" and Counterparty agrees, and Counterparty

shall procure that Authorized Party (as applicable) agrees before providing any Counterparty Personal Data, that it is the "data exporter" under the SCCs 2021.

8.3. UK Data Transfers. By entering into the Agreement, the Parties enter into the SCCs 2010, which are hereby incorporated by reference forming an intergral part of this DPA and available at https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:EN:PDF in order to provide appropriate safeguards with regard to Counterparty Personal Data in case of transfers outside of the UK to a Third Country.
Appendix 1 of the SCCs 2010 is replaced by Annex I.A. and I.B. of the SCCs 2021, and Appendix 2 of the SCCs 2010 is replaced by Annex II of the SCCs 2021.

9. Return or Deletion of Counterparty Personal Data

9.1. The instructions related to returning or deleting Participant Personal Data are set forth in the Agreement.

10. Limitation of Liability

10.1. Sensitive Data. The Parties shall ensure that any B2B Personal Data exchanged between the Parties do not include Sensitive Data. Thus, neither Party will have a liability towards the other Party or any other person whatsoever for Sensitive Data. If there is Security Incident related to Personal Data that was provided in contravention of this Section 10.1, under no circumstances will the receiving Party be liable for disclosure of such information and the Party that provided the Personal Data in question will fully release, indemnify and hold harmless the receiving Party from and against any liability, loss, claim, demand, cost and expense arising out of any such processing of Sensitive Data, including Security Incidents.

10.2. Participant Personal Data. As R3 does not determine the purposes or the means of the processing of Counterparty Personal Data, under no circumstances will R3 be liable for any such processing. Counterparty and Authorized Party (as applicable) shall fully release, indemnify and hold harmless R3 from and against any liability, loss, claim, demand, cost and expense arising out of any processing related to Counterparty Personal Data.

10.3. Each Party's liability taken together in the aggregate arising out of or related to this DPA (including the SCCs 2010 and SCCs 2021) shall be subject to the exclusions and limitations of liability set forth in the Agreement.

10.4. Any claims against R3 under or in connection with this DPA (including, where applicable, the SCCs 2010 and SCCs 2021) shall be brought solely against the entity that is a party to the Agreement.

10.5. In no event shall any Party limit its liability with respect to any individual's data protection rights under this DPA or otherwise.

11. Relationship with the Agreement

11.1. This DPA shall remain in effect for as long as R3 carries out Counterparty Personal Data processing operations on behalf of Counterparty or Authorized Party (as applicable) or until termination of the Agreement.

11.2. The Parties agree that this DPA shall replace any existing data processing agreement or similar document that the Parties may have previously entered into in connection with the Agreement.

11.3. In the event of any conflict or inconsistency between this DPA and the Agreement, the provisions of the following documents (in order of precedence) shall prevail: (a) SCCs 2021 and (b) SCCs 2010; then (c) this DPA; and then (d) the Agreement.

11.4. Except for any changes made by this DPA, the Agreement remains unchanged and in full force and effect.

11.5. No one other than a party to the Agreement, its successors and permitted assignees shall have any right to enforce any of its terms.

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

Exhibit A: Standard Contractual Clauses (processors) for transfers out of the EEA

For the purposes of Article 46.2.(c) of the GDPR for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Counterparty or Authorized Party (as applicable),

(the data **exporter**)

And R3,

(the data **importer**)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Annex 1.B.

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:

[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 […].

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

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

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

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

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

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

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 - Clause 8.1(b), 8.9(a), (c), (d) and (e;

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

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

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18 - Clause 18(a) and (b).

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

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7

Docking clause

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

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

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

8.1 Instructions

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

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

8.2 Purpose limitation

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

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the 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.

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

[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.

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 30 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

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

law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

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

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

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

Clause 11

Redress

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

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

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

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

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

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

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

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

Clause 12

Liability

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

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

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

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

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

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

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

Clause 13

Supervision

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

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article

3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

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

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

(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.

[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.

Clause 15

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

15.1 Notification

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

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

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

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

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

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

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

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to

do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

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

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

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

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

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

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

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

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

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

to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

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

Clause 17

Governing law

These Clauses shall be governed by the law of 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 Ireland.

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 Ireland.

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

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

APPENDIX TO THE STANDARD CONTRACTUAL CLAUSES

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: …

Address: …

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

Activities relevant to the data transferred under these Clauses: …

Signature and date: …

Role (controller/processor): …

2. …

Data importer(s):

1. Name: R3

Address: as indicated in the Agreement.

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

Activities relevant to the data transferred under these Clauses: as indicated in the Agreement.

Signature and date: ……

Role (controller/processor): processor.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Individuals whose Personal Data are provided by Counterparty or Authorized Party (as applicable) as Counterparty Personal Data.

Categories of personal data transferred

Personal Data provided by Counterparty or Authorized Party (as applicable) as Counterparty Personal 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.

N/A

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

Data is transferred on a continuous basis for the duration of the Agreement.

Nature of the processing

As indicated in the Agreement.

Purpose(s) of the data transfer and further processing

As indicated in the Agreement.

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

As indicated in the Agreement.

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

See list [https://www.r3.com/Sub-Processors-List]

C. COMPETENT SUPERVISORY AUTHORITY

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

Ireland

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

1. Organizational Security Controls

R3 will implement and maintain technical and organizational measures to protect Counterparty Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access as described below ("Security Measures"). The Security Measures include governance around access to systems storing Counterparty Personal Data; to help restore timely access to Counterparty Personal Data following a Security Incident; and for regular testing of effectiveness. R3 will maintain such Counterparty Personal Data according to the control framework defined by R3's information security management framework.

a. Security Compliance

R3 will take appropriate steps to require compliance with Security Measures by its employees, contractors and other processors to the extent applicable to their scope of performance, including ensuring that all persons authorized to process Counterparty Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

b. Data Incidents

If R3 becomes aware of any Security Incidents, R3 will follow steps outlined above in section 6.4 of the DPA on the Security Incident response.

c. Security Responsibility

R3's information security manager is responsible for ensuring the Security measures described herein.

2. Technical Security Controls

a. Access Policy

R3's internal access control processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process Counterparty Personal Data. R3's information security manager only provides authorized users with access to Counterparty Personal Data and all users are allocated unique user IDs for access to systems processing Counterparty Personal Data.

b. Data

Production systems containing Counterparty Personal Data will be logically segregated from development systems. Appropriate authentication schemes will be maintained for systems processing Counterparty Personal Data. Systems processing Counterparty Personal Data will adequately protect that information at rest and in transit. Counterparty Personal Data will be deleted in accordance to with section 9 of the DPA on Return or Deletion of Counterparty Personal Data.

c. Other processors' Security

R3 reviews security and privacy practices of other processors to require such other processors to provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide.