DATA PROCESSING AGREEMENT

1. Definitions

1.1 The following definitions apply for the purposes of this Data Processing Agreement (DPA):

"**Applicable Data Protection Laws**" means: (i) the General Data Protection Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 ("**GDPR**") on the protection of natural persons with regard to the Processing of personal data and on the free movement of such data; (ii) the UK Data Protection Act 2018"" ("**UK GDPR**"); and (iii) any law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding restriction (as amended, consolidated, re-enacted or replaced from time to time) which relates to the protection of individuals with regards to the Processing of Personal Data to which a party to this DPA is subject;

"**Audit**" as described in Clause 3 of this DPA;

"Controller", "Processor", "**Data Subject**", "**Personal Data**", "**Process**", "**Processed**" **or** "**Processing**" shall each have the meanings given in Applicable Data Protection Law. If and to the extent that Applicable Data Protection Laws do not define such terms, then the definitions as set out in the GDPR. The types of Personal Data are detailed in Exhibit A attached hereto;

"**Security Incident**" means an unauthorized, or unlawful access to, use of, or disclosure of Personal Data which is Processed by Digital Realty in connection with this DPA;

"**Standard Contractual Clauses**" means (i) where the GDPR applies, the standard contractual clauses for the transfer of Personal Data to Third Countries pursuant to the European Commission's decision 2021/914/EC of June 4, 2021, as may be updated from time to time (the "**EU SCCs**"); (ii) where the UK GDPR applies, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, in force 21 March 2022, as may be updated from time to time (the "**UK SCCs**"); (iii) where the Swiss DPA applies, the applicable standard data protection clauses issued, approved or recognised by the Swiss Federal Data Protection and Information Commissioner as may be updated from time to time (the "**Swiss SCCs**"); (iv) and any other applicable standard data protection clauses which relates to the protection of individuals with regards to the Processing of Personal Data to which a party to this DPA is subject. "**Third Country(ies)**" means (i) in relation to Personal Data transfers subject to the GDPR, any country outside of the scope of the data protection laws of the European Economic Area, excluding countries approved as providing adequate protection for Personal Data by the European Commission from time to time; and (ii) in relation to Personal Data transfers subject to the UK GDPR, any country outside of the scope of the data protection laws of the UK, excluding countries approved as providing adequate protection for Personal Data by the relevant competent authority of the UK from time to time.

2. Relationship of the Parties

2.1 Customer and Digital Realty shall comply with Applicable Data Protection Laws. Where Digital Realty provides Personal Data to Customer concerning Digital Realty's employees, contractors, and other personnel, Customer agrees to process such information solely for the purposes of carrying out the engagement as set forth under the Agreement. Customer shall use reasonably appropriate administrative, technical, and organizational safeguards to ensure the security and confidentiality of such Personal Data.

2.2 Customer and Digital Realty acknowledge and agree that with regard to the Processing of Personal Data associated with the purposes and processing activities as described in Digital Realty's Privacy Practices at https://www.digitalrealty.com/privacy and as may be updated from time to time and limited to processing in the context of Digital Realty's customer portals and data center remote hands services, Customer is the Controller, Digital Realty is a Processor and that Digital Realty may engage sub-processors pursuant to the requirements set forth below.

2.3 Customer and Digital Realty acknowledge and agree that regarding the Processing of Personal Data in the context of maintaining Digital Realty's data center services, including all physical security and facilities access control provisioning as described in Digital Realty's Privacy Practices at https://www.digitalrealty.com/privacy, Customer may act either as a Controller or Processor and Digital Realty is an independent Controller, not a joint controller with Customer. Where Digital Realty is an independent Controller, only Section 4 of this DPA shall apply (sections 3 and 5 do not apply).

2.4 Customer shall ensure that its instructions comply with all Applicable Data Protection Laws in relation to the Personal Data, and that the Processing of Personal Data in accordance with Customer's instructions and the terms of this DPA will not cause Digital Realty to be in breach of the Applicable Data Protection Laws. Customer is solely responsible for the accuracy, quality, and legality of (i) the Personal Data provided to Digital Realty by or on behalf of the Customer; (ii) the means by which Customer acquired any such Personal Data; and (iii) the instructions it provides to Digital Realty regarding the Processing of such Personal Data. Customer has provided notice and obtained, or will obtain, all consents and rights necessary under Applicable Data Protection Laws for Digital Realty to process Personal Data and provide the Services pursuant to the Agreement.

3. Digital Realty's Obligations

3.1 To the extent Digital Realty Processes Personal Data on behalf of Customer, it shall:

3.1.1 Process the Personal Data only on documented instructions from Customer, including with regard to transfers of Personal Data to Third Countries or an international organisation, unless required to Process such Personal Data by Union or Member State law to which Digital Realty is subject; in that case, Digital Realty will inform Customer of that legal requirement before Processing, unless that law prohibits this information on important grounds of public interest;

3.1.2 ensure that its personnel authorised to Process the Personal Data are under an appropriate contractual or statutory obligation of confidentiality;

3.1.3 implement appropriate technical and organisational security measures that will meet or exceed the requirements set forth in Schedule 2 to this DPA;

3.1.4 taking into account the nature of the Processing, assist Customer by implementing appropriate technical and organisational measures, to the extent that this is possible, for the fulfilment of Customer's obligation to respond to requests for exercising the Data Subject's rights laid down in the Applicable Data Protection Laws;

3.1.5 without undue delay, notify Customer in writing upon becoming aware of any confirmed unauthorized, or unlawful access to, use of, or disclosure of Personal Data which is Processed by Digital Realty in connection with this DPA (a "**Security Incident**"). Digital Realty will provide Customer with information necessary for Customer' to fulfil its obligations pursuant to Applicable Data Protection Laws. Notification in accordance with this section will not be construed as an acknowledgement by Digital Realty of any fault or liability with respect to the Security Incident;

3.1.6 assist Customer in ensuring compliance with the obligations to (i) implement appropriate technical and organisational security measures; (ii) notify (if required) Security Incidents to applicable regulators and/or individuals; and (iii) conduct data protection impact assessments and, if required, prior consultation with applicable regulators;

3.1.7 at the choice of Customer, delete or return all the Personal Data to Customer after the end of the provision of services relating to Processing, and delete existing copies of the Personal Data unless Union or Member State law requires storage of the Personal Data;

3.1.8 make available to Customer all information necessary to demonstrate compliance with the obligations laid down in this clause 3 and Applicable Data Protection Laws, and allow for and contribute to audits, including inspections, conducted by Customer or another auditor mandated by Customer. Customer will notify Digital Realty at least ten (10) business days in advance of Customer's desire to perform an audit. Any such audit will be conducted at Customer's expense (including reasonable fees and expenses to compensate Digital Realty for its time and out of pocket costs involved in responding to any audit request) no more than once annually, and will be limited to what is reasonably necessary to verify Digital Realty's compliance with this DPA, must occur during Digital Realty's normal business hours, and must otherwise be consistent with the requirements of this Section.

3.2 Digital Realty will immediately inform Customer if, in Digital Realty's opinion, an instruction of Customer infringes the Applicable Data Protection Laws.

4. International Transfers

4.1 The Customer acknowledges and agrees that Digital Realty may appoint an affiliate or third party sub-processor to Process Customer's Personal Data in a Third Country, as long as it ensures that such Processing takes place in accordance with the requirements of Applicable Data Protection Laws.

4.2 To the extent that Digital Realty Processes Personal Data in a Third Country and is acting as a data importer, Digital Realty shall comply with the data importer's obligations and Customer shall comply with the data exporter's obligations as set out in the applicable Standard Contractual Clauses which are hereby incorporated into and form part of this DPA and completed as follows:

4.2.1 Module One (Controller to Controller) of the EU SCCs will apply in those situations described in Section 2.3;

4.2.2 Module Two (Controller to Processor) will apply in those situations described in Section 2.2;

4.2.3 Annex I shall be deemed completed with the information set out in Schedule 1, as applicable;

4.2.4 Annex II shall be deemed completed with the information set out in Schedule 2;

4.2.5 if applicable, for the purposes of (i) Clause 7, the optional docking clause will not apply (ii) Clause 9, Option 2 (General Written Authorization) is deemed to be selected and the notice period specified in Section 5.1 of this DPA shall apply; (iii) Clause 11(a), the optional wording in relation to independent dispute resolution is deemed to be omitted; (iv) Clause 13 and Annex I.C., the competent supervisory authority shall be the Autoriteit Persoonsgegevens; (vi) in Clause 17 Option 1 is deemed to be selected and the governing law shall be the Netherlands (v) Clause 18, the competent courts shall be of the Netherlands.

4.2.6 For data transfers subject to the UK SCCs, the UK SCCs are hereby incorporated into and form part of this DPA and completed as follows: (i) in Table 1 of the UK SCCs, the parties' details and key contact information is located in Section A of Schedule 1 of this DPA; (ii) in Table 2 of the UK SCCs, information about the version of the Approved EU SCCs, the modules and selected clauses to which this UK International Data Transfer Agreement is appended to is located in Section 4.2 of this DPA (iii) In Table 3 of the UK SCCs (A) the list of Parties is located in Section A of this Schedule 1; (B) the description of the transfer is set forth in Section B of Schedule 1 (Details of the Processing); (C) Annex II is located in Schedule 2; (D) the list of sub-processors is located at www.digitalrealty.com/sub-processor; (iv) in Table 4 of the UK SCCs, both the importer and the exporter may end the UK SCCs in accordance with the terms of the UK SCCs.

4.2.7 In case of any transfers from Switzerland, (i) general and specific references in the EU SCCs to GDPR or EU or Member State Law shall have the same meaning as the equivalent reference in the Data Protection Laws of Switzerland, as applicable; and (ii) any other obligation in the EU SCCs determined by the Member State in which the data exporter or Data Subject is established shall refer to an obligation under Swiss DPA, as applicable. To extent that and for so long as the EU SCCs as implemented in accordance with this DPA cannot be relied on by the parties to lawfully transfer Personal Data in compliance with the applicable standard data protection clauses issued, adopted or permitted under Swiss DPA shall be incorporated by reference, and the annexes, appendices or tables of such clauses shall be deemed populated with the relevant information set out in Schedules 1 and 2 of this DPA.

5. Sub-Processing

5.1 Customer hereby acknowledges and agrees that Digital Realty may engage (i) Digital Reality affiliates as sub-processors; and (ii) the sub-processors set out at https://www.digitalrealty.com/about/legal/privacy/sub-processors. Customer acknowledges and agrees that the other party may engage third-party Sub-processors in connection with the provision of the Services. That other Party will enter into a written agreement with each Sub-processor containing data protection obligations that provide at least the same level of protection for Personal Data as those in this DPA, to the extent applicable to the nature of the Services provided by such Sub-processor.

5.2 Customer hereby consents to this list of sub-processors, their locations, and processing activities as it pertains to its Personal Data. Digital Realty shall: (A) make available an up-to-date list of the sub-processors it has appointed upon written request from Customer; and (B) notify Customer if it adds any new sub-processors at least 14 days prior to allowing such sub-processor to process Customer Personal Data. Customer may request the current list of Sub-processors for the Services, including the identities of those Sub-processors and their country of location via email from Privacy@digitalrealty.com. Customer will have 14 days from the date of receipt of the notice to approve or reject the change. If Customer does not object in this time period, the sub-processor will be deemed accepted. If Customer rejects the replacement sub-processor, Digital Realty may terminate the services relying on the replacement sub-processor with immediate effect on written notice to Customer.

5.3 Digital Realty is responsible under the Applicable Data Protection Laws for the acts or omissions of its sub-processors to the same extent it would be liable if performing the Services of each Sub-processor directly under the terms of this DPA. Digital Realty will impose data protection obligations upon any sub-processor that are no less protective than those included in this DPA.

This DPA may be executed electronically and in any number of counterparts, each of which is an original and all of which evidence the same agreement between the parties. Except for matters covered by this DPA, this DPA is subject to the terms of the Agreement. Except as specifically amended and modified by this DPA, the terms and provisions of the Agreement remain unchanged and in full force and effect. The exclusions and limitations on liability contained in the Agreement shall apply to any liability arising under or in respect of this DPA. The terms of this DPA will control to the extent there is any conflict between terms of this DPA and the terms of the Agreement. If there is any conflict between this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses will prevail with respect to Personal Data that is subject to EU GDPR or UK GDPR.

IN WITNESS WHEREOF, each party has caused this DPA to be signed and delivered by its duly authorized representative.

CUSTOMER

Signature:
Name: Jack Twomey
Title: Managing Director
Date: 6.3.2024

DIGITAL REALTY

DocuSigned by:
Séamus Dunne
A6A1B4F2CA134AB...
Signature:
Name: Séamus Dunne
Title: MD
Date: March 14, 2024

SCHEDULE 1 – Details of Processing

Section A: List of Parties

Data Importer: Digital Realty

Address:

5707 Southwest Parkway
Building 1, Suite 275
Austin, TX 78735

Contact person's name, position and contact details:
Jeannie Lee, General Counsel
privacy@digitalrealty.com

Role: Processor/Controller

Data Exporter: Cloud2Me Ltd

Address:

OldPost,
19 High Street, Nutfield,
Surrey, RH1 4HH, England

Contact person's name, position and contact details:
Jack Twomey, Managing Director
jack.twomey@cloud2me.co.uk

Role: Controller

Section B: Description of Processing/Transfer

- **Categories of data subjects whose personal data is transferred**

  Employees, personnel, or other contact persons of Digital Realty or Customer.

- **Categories of personal data transferred**

  Contact and portal access data:

  - Contact data such as individuals' names, title/position in the company, business addresses, business or mobile telephone numbers, or business email addresses
  - Access credentials (user ID and password) for accessing our Portals and/or systems
  - Work order details (records of work orders placed on our Portals) and other business-related personal information shared with Digital Realty in a work order or in the course of provisioning a service
  - Records of consent you have given, together with date and time, means of consent and any related information (e.g., subject matter of consent)
  - Cookie and analytics data including
    - Device type, operating system, browser type, browser settings, IP address, language setting, dates, and times of connecting to a website
    - Records of your interactions with our online advertising and content, any interaction you may have with such content or advertising (e.g., mouse hover, mouse clicks, any forms you complete in whole or in part) and any touchscreen interactions
    - Portal usage statistics, Portal settings, dates and times of connecting to a Portal, username, password, security login details, usage data, aggregate statistical information

  Personal data necessary for security and physical access to our facilities:

  - Individuals' names, [government approved] personal identification, vehicle registration number subject to applicable law
  - Data center access records, including dates, times, locations of individuals' physical access, and any location data or biometric data subject to local requirements
  - CCTV footage and images of individuals near, entering, or inside our facilities

- **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.**

Customers are prohibited from providing such information.

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

  Transfers will be continuous for the duration necessary for the performance of the Services; any other purposes stipulated in the Agreement or any applicable SOW; and complying with applicable laws and regulations;

- **Nature of the processing**

  Customer Personal Data will be subject to those Processing operations described in the Agreement, which may include: ‘Remote Hands’ or similar services; storage of media (e.g. back up tapes) which contain Personal Data, and disposal of hardware and media including wiping of Personal Data; and access to hardware on which Personal Data is stored to perform hardware maintenance.

- **Purpose(s) of the data transfer and further processing**

  Customer Personal Data will be subject to those Processing operations described 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**

  In the course of providing such services to Customer, Vendor will, for the duration set out in the Agreement, Process Customer Personal Data as instructed by Customer.

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

  All authorized sub-processors are required to implement and maintain the same or substantially similar technical and organizational measures, responsibilities and obligations as those required of Digital Realty under this DPA.

Section C: Competent Supervisory Authority

The Netherlands, Autoriteit Persoonsgegevens

SCHEDULE 2 – Security Measures

SCHEDULE 2 – Security Measu

1. Program. When acting as a Processor, the processing party will implement and maintain a comprehensive written information security program ("**Information Security Program**"), which contains appropriate administrative, technical and organizational safeguards that comply with this Schedule B and that: (a) addresses the security, integrity, availability, resilience and confidentiality of Personal Data; (b) mitigates the risk of a Personal Data Breach; and (c) meets or exceeds prevailing industry standards.

2. Access Controls. When acting as a Processor, the processing party will implement measures to: (a) abide by the "principle of least privilege," pursuant to which access to Personal Data by the processing party's personnel will limited on a need-to-know basis; (b) verify the reliability of personnel accessing Personal Data prior to providing such access; (c) provide appropriate security training to such personnel; and (d) promptly terminate its personnel's access to Personal Data when such access is no longer required for performance under the Arrangement.

3. Account Management. When acting as a Processor, the processing party will manage the creation, use, and deletion of all account credentials used to access the processing party's network, including by requiring unique credentials for each user and by implementing minimum password length and format requirements to ensure strong passwords.

4. Vulnerability Management. When acting as a Processor, the processing party will: (a) periodically use automated vulnerability scanning tools to scan its production system for vulnerabilities; and (b) implement patch management and software update tools as made available by the providers of those tools.

5. Security Segmentation. When acting as a Processor, the processing party will monitor, detect and restrict the flow of information on a multilayered basis using tools such as firewalls, proxies, and network-based intrusion detection systems.

6. Data Loss Prevention. When acting as a Processor, the processing party will use loss prevention measures to identify, monitor and protect Personal Data in use, in transit and at rest. Such data loss prevention processes and tools will include: (a) automated tools designed to identify attempts of data exfiltration; and (b) use of certificate-based security.

7. Encryption. When acting as a Processor, the processing party will encrypt, using industry standard encryption tools, all Personal Data that it: (i) transmits or sends wirelessly or across public networks; (ii) stores on laptops or storage media, and (iii) stores on portable devices or within its network, computers, software or systems.

8. Pseudonymization. When acting as a Processor, the processing party will, where possible and consistent with the Services, use industry standard pseudonymization techniques to protect Personal Data.

9. Physical Safeguards. When acting as a Processor, the processing party will maintain physical access controls to secure its owned physical premises where the relevant computing environment used to Process any Personal Data is located, including an access control system that enables it to control physical access to each of its facilities.