REAL ESTATE SOFTWARE

DATA PROTECTION AND SECURITY SCHEDULE

This Data Protection and Security Schedule is entered into between MRI Software EMEA Limited ("MRI") and the Client outlined in the Order Document, and the authorized representatives of the Parties hereby execute this Schedule to be effective as of the 1 November 2020, as defined in the Order Document. This Schedule is incorporated by reference into the Master Agreement dated 1 July 2018 between the Parties along with all associated schedules and order documents (the "Agreement"). Capitalized terms not defined herein shall have the meaning set forth in the Agreement. In case of any conflict or inconsistency between the provisions of this Schedule and the main terms of this Agreement, the provisions contained in this Schedule shall prevail to the extent of the inconsistency, provided always that nothing in this Schedule shall permit MRI (or any sub-Processor) to handle Personal Data in a manner which is prohibited by this Agreement or by applicable law.

1. **Security Generally.** MRI shall ensure that it has in place appropriate technical and organizational measures to protect against unauthorized or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to the Personal Data, which are appropriate to the harm that might result from the unauthorized or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures. During the Term of the Agreement, MRI shall maintain a documented information security plan ("Information Security Program"). MRI agrees to comply with all of its own requirements contained in such Information Security Program. MRI's Information Security Program shall include, at a minimum, appropriate controls and measures in relation to: (1) physical security at all MRI locations involved in the provision of the Services; (2) technical security with respect to the Client Data in MRI's possession; (3) organizational security arrangements regarding the employees and other representatives of MRI, its Affiliates, and its subcontractors, including training and awareness, staff vetting procedures and other security measures (e.g. use of passwords and security credentials); (4) encryption of Client Data contained within the SaaS Services; (5) Disaster Recovery and Business Continuity; (6) Vulnerability Testing and Security Audit; and (7) Data Breach Procedures. Additionally, MRI's Information Security Program shall comply with all laws applicable to MRI related to its security programs. MRI may update its Information Security Program from time to time in its sole discretion. Upon the occurrence of a disaster, MRI must evaluate the cause of the disaster as soon as possible, attempt to remediate the cause, and, if the outage will be sustained or cannot be remediated promptly, take appropriate actions to minimize the impact of the Disaster to the Client, such as implementing the Disaster Recover/Business Continuity Plan. Client shall not be charged an additional fee for any disaster recovery services, including backups and database restorations, performed by MRI due to a Disaster (whether at the MRI hosting location, within the SaaS Services or otherwise). MRI shall evaluate the effectiveness of its Information Security Program on a commercially reasonable periodic basis, but no less frequently than annually and (if it, acting reasonably, considers it necessary to do so) update the same.

2. **Encryption and Anonymization.** MRI shall implement and maintain, during the Term of the Agreement, encryption standards which are appropriate given the nature, scope, and purpose of the Client Data being processed. MRI may choose to utilize, in addition to or in place of the encryption standards, anonymization and pseudonymisation techniques to protect the security and confidentiality of the Personal Data (as defined below).

3. **Disaster Recovery and Business Continuity.** MRI shall implement and maintain a disaster recovery plan with contingency measures as are reasonable within its industry in light of the sensitivity of the Services which MRI provides (the "Disaster Recovery/Business Continuity Plan"). Upon the occurrence of a Disaster, MRI must promptly evaluate the cause of the Disaster, attempt to remediate the cause and, if the outage will be sustained or cannot be remediated promptly, then it will promptly implement the Disaster Recovery/Business Continuity Plan. Client shall not be charged an additional fee for any disaster recovery services, including backups and database restorations, performed by MRI due to a Disaster (whether at the MRI hosting location, within the SaaS Services or otherwise).

   MRI shall evaluate the effectiveness of its Disaster Recovery/Business Continuity Plan on a commercially reasonable periodic basis, but not less frequently than annually. MRI may modify the Disaster Recovery/Business Continuity Plan from time to time, in its sole discretion, provided that such modifications do not materially and negatively modify the services provided in the Disaster Recovery/Business Continuity Plan as of the execution of this Agreement.

4. **Vulnerability Testing and Security Audit.** MRI shall conduct regular penetration and vulnerability testing of its information technology infrastructure and networks, at a commercially reasonable frequency. Upon Client's request, MRI shall provide a letter of attestation to Client that the testing occurred. MRI may modify the scope of such penetration and vulnerability testing provided however, that the scope shall not materially and negatively change from the execution of this Agreement. During the Term of the Agreement, MRI shall comply with industry standard practices for audit and security procedures.

5. **Data Breach.** MRI will take commercially reasonable, but not less than industry standard, measures to protect the security of such Personal Data transferred by Client to MRI. In the event that MRI becomes aware or reasonably suspects that a Data Breach involving Client Personal Data has occurred, MRI will without undue delay: (i) investigate the cause of the Data Breach; (ii) notify Client of the Data Breach and provide sufficient information to allow the Client to report the Data Breach and/or notify the data subject, if required; (iii) contain and remedy any Data Breach; (iv) take reasonable steps to mitigate the effects of and to minimize any damage resulting from the Data Breach; (v) reasonably assist Client in remediating or

mitigating any potential damage from a Data Breach to the extent that such remediation or mitigation is within MRI's control; (vi) take reasonable steps to restore the security and integrity of any Systems used by MRI and/or its subcontractors to provide the Services; (vii) if the Data Breach resulted from Client's own actions the Client shall immediately on demand indemnify MRI for any costs incurred in relation to undertaking any of the foregoing and shall further indemnify MRI for all and any costs, losses, damages, expenses or otherwise incurred by MRI to the extent that the same arise from such actions of the Client.

MRI shall promptly inform Client if it receives, from a data subject whose Personal Data is the subject of the provision of Services to the Client under this Agreement, a complaint or request relating to either Party's obligations under applicable law relevant to this Agreement, including any claim from a Data Subject or any notice, investigation or other action from a regulatory authority and provide Client with details of such complaint or request.

For the purposes of this Section, **"Data Breach"** shall mean a breach of security resulting from an act or omission by MRI, its employees or its subcontractors, leading to an accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed. For the purposes of this Agreement, **"Personal Data"** shall mean any information relating to an identified or identifiable natural person (**'Data Subject'**); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person which is provided by the Client to MRI. The business information of the Client is not by itself deemed to be Personal Data. Personal Data is deemed to be Confidential Information of Client and is not Confidential Information of MRI. MRI shall reasonably cooperate with any remediation efforts undertaken by Client to correct, delete, modify, or hold Personal Data of the Data Subjects. Data Subjects may include customers of the Client, employees, and staff and contractors of the Client.

6. **Personal Data**. In addition to the terms and conditions set forth in the Agreement, Client agrees to only input into, transfer into the MRI Software and SaaS Services or provide access to MRI such Personal Data if and to the extent that it is necessary to enable MRI to provide the Services under this Agreement, and to do so only in fields specifically designed to house such Personal Data. Client is responsible for removing any Personal Data from its database(s) once it is no longer necessary for that purpose. MRI shall have no liability to Client, and Client shall indemnify MRI for all claims by third parties resulting from Client's storing Personal Data in non-designated fields. Client Personal Data shall mean Personal Data provided to MRI by the Client.

   If MRI processes personal data in the European Economic Area ("EEA"), then it must not transfer or access (or permit the transfer or access of) such Client Personal Data outside of the EEA unless: (a) the recipient of such Personal Data has first entered into a data transfer agreement with MRI containing the standard contractual clauses for the transfer of Personal Data from data processor to data processors in jurisdictions outside the EEA, adopted by the European Commission pursuant to Decision 2010/87/EU, as amended or replaced from time to time; (b) the recipient is located in a jurisdiction in respect of which the European Commission has issued a finding of the adequacy of the protection of Personal Data and the rights and freedoms of individuals; (c) the recipient qualifies under Chapter 5 of GDPR; or (d) MRI is able to demonstrate to the Client's reasonable satisfaction that the transfer otherwise satisfies the requirements of the applicable data protection and privacy laws and regulations.

7. **Additional definitions:**

   "Applicable Law" means: (a) any statute, regulation, by law, ordinance or subordinate legislation in force from time to time to which a Party to this Agreement is subject insofar as the same relates to that Party's performance under this Agreement; the common law as applicable to the Parties to this Agreement from time to time, including European Union laws or the laws of the European member state to which MRI is subject; (b) any binding court order, judgment or decree given in respect of either party; (c) any applicable industry code, or standard enforceable by law; and (d) any applicable direction, rule or order that is binding on a Party hereto and that is made or given by anybody having jurisdiction over a Party or any of that party's assets, resources or business.

   "Controller" means the natural or legal person which determines (individually or jointly or in common with others) the purposes for which and the manner in which any Client Personal Data are or will be Processed. For the purposes of this Agreement, the Client shall be deemed the Controller.

   "Data Protection Legislation" means any Applicable Law relating to the Processing, privacy, and use of Personal Data including, without limitation: (i) EU Council Directives 95/46/EC and 2002/58/EC; (ii) the Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) ("GDPR"); (iii) any corresponding or equivalent national laws or regulations; or (iv) approved codes of conduct or approved certification mechanisms issued by any relevant regulatory authority.

"Data Protection Losses" means all liabilities and amounts, including all: (a) costs (including legal costs), claims, demands, actions, settlements, losses, liabilities and damages; (b) to the extent permitted by Applicable Law: (i) administrative fines, penalties, imposed by a regulatory authority; (ii) compensation to a data subject ordered by a regulatory authority; and (iii) the reasonable costs of compliance with investigations by a regulatory authority; and (c) the costs of loading Client Personal Data and replacement of Client materials and equipment, to the extent the same are lost, damaged or destroyed, and any loss or corruption of Client Personal Data including the costs of rectification or restoration of Client Personal Data.

"Processing" means any operation or set of operations which is performed on Personal Data or 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, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction and **"Process"** and **"Processed"** will be interpreted accordingly.

"Processing Instructions" means the written instructions for Processing Client Personal Data, as set out in this Schedule and in the Agreement, including this Schedule, and otherwise as provided in writing by or on behalf of Client to MRI or a MRI Affiliate from time to time.

"Processor" means the natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller. For the purposes of this Agreement, MRI shall be deemed the Processor.

"Subprocessor" means any third party engaged by MRI to Process Client Personal Data on behalf of MRI.

8. **Data Processing**. As Processor, MRI will only act upon and Process Client's Personal Data for the purposes of performing its obligations under the Agreement, subject to the Processing Instructions. Personal Data will be used by MRI in accordance with and for the purposes set out in the Processing Instructions and only where reasonably necessary to provide the Services to Client. Client's instruction to cease Processing Client Personal Data shall not alleviate Client's obligations under the Agreement, including without limitation, its payment obligations.

   Additionally, MRI shall be permitted to Process Client Personal Data, without regard for the Processing Instructions, if required to do so by Applicable Law; in such case, MRI shall promptly notify the Client of that legal requirement before Processing, unless that law prohibits such notification. If MRI is ever unsure as to the parameters or lawfulness of the Processing Instructions issued by Client, MRI will, as soon as reasonably practicable, revert to Client.

   MRI shall comply with its obligations as a Processor under the applicable Data Protection Legislation in relation to the Processing of Client Personal Data by it under this Agreement.

   MRI shall reasonably cooperate and provide information to the Client in order to assist the Client in completion of its data protection impact assessments (**"DPIAs"**) and shall reasonably provide consultations with (or notifications to) relevant regulators which are necessary pursuant to Data Protection Legislation in relation to the Personal Data and the Services. For clarification purposes, the Parties acknowledge that the scope of the Services contemplated herein as of the execution of the Agreement are not of the type which would likely necessitate a data protection impact assessment by the Controller.

   MRI may forward to the Client any requests from Data Subjects in respect of Client Personal Data pursuant to Data Protection Legislation (including the ability to correct, delete, block or port Client Personal Data and rights of access) and reasonably cooperate with the Client in complying with any such Data Subject's exercise of his/her rights in relation to such Personal Data as is Processed by MRI. Client may be required to make such requested modifications itself within the MRI system. MRI may respond directly to and action any request from Data Subjects with respect to information to which it is the Controller.

   MRI shall maintain such records and information as are necessary to demonstrate its compliance with Data Protection Law in relation to the Processing of Client Personal Data on behalf of Client under this Agreement, containing as a minimum the information required under Data Protection Legislation, which shall be made available to Client upon request.

   MRI shall reasonably cooperate with the Client in good faith to ensure compliance with its obligations under the Data Protection Legislation in respect of Client Personal Data taking into account the nature of Processing and the information available to MRI.

9. **Duration of Processing**. Processing of the Client Personal Data by MRI shall be for the Term of this Agreement, subject to restrictions outlined by Applicable Law. The Parties acknowledge that Personal Data is provided to MRI by the Client and Client shall be responsible for removing and deleting such Personal Data from the SaaS Services when such Personal Data is no longer necessary for the purpose for which is was collected. The Parties agree that the Personal Data, may be held in back up and not accessed, except at the consent of the Controller, for a reasonable amount of time following the expiration of the Term.

10. **Scope of Personal Data**. Client may provide and MRI may process the following types/categories of Personal Data for the following categories of Data Subject:

Type of Data	Data Subjects Impacted
Personal Information; Contact Details; Financial or Payment Details; Files, Images, or Videos; Contractor Insurance Information Contractor CIS information VAT information	Customers (Owners/Companies) Client's customers (tenants/residents); Client's employees and staff; Suppliers

11. **MRI personnel**. MRI shall ensure that its personnel will not Process Client Personal Data: (i) except in accordance with the provisions of this Schedule; and (ii) procure that personnel are contractually obligated to maintain the security and confidentiality of any Client Personal Data. MRI shall take reasonable steps to ensure that the personnel Processing Client Personal Data receive adequate training on compliance with this Agreement and the Data Protection Legislation applicable to the Processing.

12. **Subprocessor.** The Client consents to MRI's use of its current Subprocessors, which is available on MRI's Privacy Policy (https://www.mrisoftware.com/uk/privacy-policy/). If MRI intends to appoint any further third-party Processor of the Client Personal Data, or change, or add to, the location(s) at which any of the Subprocessors Processes Client Personal Data or the Software made available to the Client, it may do so: (i) with the Client's prior consent; or (ii) without the Client's prior approval, provided that MRI shall:(a) provide prior notice to the Client by posting such updates to MRI's Privacy Policy; (b) carry out adequate due diligence to ensure that the Sub-contractor is capable of providing the level of protection for Client Personal Data required by this Agreement; (c) ensure that any additional or replacement Subprocessors shall be contractually bound to obligations with respect to the Processing of Client Personal Data substantially similar to those to which MRI is bound by this Schedule; and (d) MRI shall provide reasonable documentation to evidence its compliance with this provision to Client on request and provide reasonable cooperation and assistance to the Client in its own assessment of the new Subprocessors or the new location. Client shall have thirty (30) days from the posting of a new Subprocessor to inform MRI of its objection to the appointment of the Subprocessors. In the event that the Client shall object to any such change and the Parties do not reach a mutually acceptable position in relation to the proposed changes, MRI shall, in its sole discretion, be entitled to terminate the Agreement immediately on giving written notice to the Client.

13. **Standard Contractual Clauses**. The Standard Contractual Clauses set out in Annex A will form part of this Data Protection and Security Schedule and apply where: (i) the Client is based in the European Economic Area; and (ii) MRI as the Client's data processor transfers data from the European Economic Area to the United Kingdom, then in the circumstances where the United Kingdom does not have an 'adequacy' ruling or other confirmation that it provides an adequate level of protection for personal data from the European Commission. If the Standard Contractual Clauses apply, nothing in this Data Protection and Security Schedule varies or modifies the Standard Contractual Clauses nor affects any supervisory authority or data subject's rights under the Standard Contractual Causes. In the event that the Standard Contractual Clauses are modified by the European Commission, then Annex A shall be deemed to be updated to reflect the final modifications.

Capitalized terms not otherwise defined have the meaning set forth in the Agreement. All other provisions of the Agreement remain in full force and effect.

MRI Software EMEA Limited (formely Qube Global Software) ("MRI")
9 King St.
London, UK EC2V 8EA

("Client")

Signature: _____ Signature: _____

Print Name: _____ Print Name: _____

Title: _____ Title: _____

Annex A

Standard Contractual Clauses (Processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation:

Address:

Tel:

Fax:

Email:

Other information needed to identify the organisation:

……..……..……..……..……..……..……..……..……..……..

("the data **exporter**")

Name of the data importing organisation: MRI Software Limited

Address: 9 King Street, London, EC2V 8EA

Tel: 020 3861 7100

Fax:

Email: dataprivacypractitioner@mrisoftware.com

Other information needed to identify the organisation: CRN: 03341304

……..……..……..……..……..……..……..……..……..……..

("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 Appendix 1.

Clause 1
Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24

October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law***'** means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

  (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

  (ii) any accidental or unauthorised access, and

  (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.
   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.
3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely England.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely England.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporters:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature……

On behalf of the data importer:

Name (written out in full): Roman Telerman

Position: CFO

Address: 9 King Street, London, EC2V 8EA

Other information necessary in order for the contract to be binding (if any): CRN: 03341304

Signature……

REAL ESTATE SOFTWARE

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

The data exporter is a client of the data importer who has procured its software and/or services for real estate property management.

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

The data importer's business/organization type is IT, digital, technology and telecoms. It is a UK based supplier of real estate property management software and services which are available through on-premise, hosted and SaaS deployment methods. It is part of a wider group of companies with its ultimate parent company based in Ohio, USA.

Data subjects

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

- tenants and/or occupants of social housing
- customers and clients (including their staff)
- suppliers (incliding their staff)
- relatives, guardian and associates of the data subject
- experts and witnesses
- complainants, correspondents and enquirers
- advisers, consultants and other professional experts

Categories of data

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

- Personal details, including any information that identifies the data subject and their personal characteristics, including: name, address, contact details, age, date of birth, sex, and physical description.
- Personal details issued as an identifier by a public authority, including passport details, national insurance numbers, identity card numbers, driving licence details.

- Family, lifestyle and social circumstances, including any information relating to the family of the data subject and the data subject's lifestyle and social circumstances, including current marriage and partnerships, marital history, details of family and other household members, habits, housing, travel details, leisure activities, and membership of charitable or voluntary organisations.
- Education and training details, including information which relates to the education and any professional training of the data subject, including academic records, qualifications, skills, training records, professional expertise, student and pupil records.
- Employment details, including information relating to the employment of the data subject, including employment and career history, recruitment and termination details, attendance records, health and safety records, performance appraisals, training records, and security records.
- Financial details, including information relating to the financial affairs of the data subject, including income, salary, assets and investments, payments, creditworthiness, loans, benefits, grants, insurance details, and pension information.
- Goods or services provided and related information, including details of the goods or services supplied, licences issued, and contracts.
- Personal data relating to criminal convictions and offences including anti-social behavious

Special categories of data (if appropriate)

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

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- health
- sex life or sexual orientation
- criminal convictions and offences

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

- Receiving data, including collection, accessing, retrieval, recording, and data entry
- Holding data, including storage, organisation and structuring
- Using data, including analysing, consultation, testing, automated decision making and profiling
- Updating data, including correcting, adaptation, alteration, alignment and combination
- Protecting data, including restricting, encrypting, and security testing
- Sharing data, including disclosure, dissemination, allowing access or otherwise making available
- Returning data to the data exporter or data subject
- Erasing data, including destruction and deletion

The processor will process personal data as specified in the provision of services pursuant to the Agreement and any Order Documents.

DATA EXPORTERS

Name:……..……..……..……..…..…

Authorised Signature ……..……..……..…..…

DATA IMPORTER

Name:……..……..……..……..…..…

Authorised Signature ……..……..……..…..…

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

The technical and organizational security measures for this Appendix are specified in the Data Protection and Security Schedule forming part of the agreement for the procurement of the software/services between the Data Importer and the Data Exporter