Data Processing Addendum

This Addendum is between:

1. ARTLOGIC MEDIA LIMITED, a company registered in England and Wales with company number 03829035, whose registered office is at 1 Pickle Mews, London, SW9 0FJ ("**Artlogic**"), (the "**Provider**"); and
2. **the Client** signing this agreement (the "**Client**"),

each a "**party**" and together the "**parties**".

1. DEFINITIONS

Addendum: this Data Processing Addendum.

Agreement: the agreement between Client and Provider regarding services for which this is an addendum.

Affiliate: any company, partnership or other entity which at any time directly or indirectly controls, is controlled by or is under common control with either party including as a subsidiary, parent or holding company;

Applicable Laws: the law of the European Union, the law of any member state of the European Union and/or **Domestic UK Law**; and **Domestic UK Law** means the UK Data Protection Legislation and any other law that applies in the UK.

Data Protection Legislation: the UK Data Protection Legislation and the General Data Protection Regulation ((EU) 2016/679) (GDPR) and any other directly applicable European Union regulation relating to privacy.

Data Subject, Personal Data, Controller, Processor and other terms defined in the GDPR: have the meaning set out in Article 4(1) of the GDPR.

Restricted Transfer: a transfer of Personal Data from the Client to the Provider or from the Provider to a third-party processor, where such transfer would, in the absence of SCC or appropriate safeguards under Data Protection Legislation be prohibited by Data Protection Legislation.

Services: the services described in the Agreement.

Standard Contractual Clauses (SCC): the European Commission's Standard Contractual Clauses for the transfer of Personal Data from the European Union to processors established in third countries (controller-to-processor transfers), as set out in the Annex to Commission Decision 2010/87/EU, a completed copy of **which comprises Schedule 3 and Annexes A and B to Schedule 3**.

UK Data Protection Legislation: any data protection legislation from time to time in force in the UK including the Data Protection Act 1998 or 2018 or any successor legislation.

2. CONTENT, VARIATION AND ORDER OF PRIORITY

2.1 This Addendum consists of:

- the main body of the Addendum
- Schedules 1, 2 and Schedule 3 (including Annexes A and B)

Schedule 3 (including Annexes A and B) contains the Standard Contractual Clauses for the transfer of Personal Data from the European Union to processors established in third countries. It is necessary for every Client in the EU to create this agreement with the Provider in order for personal data to be processed in compliance with the GDPR.

2.2 This Addendum including its Schedules and Annexes varies the Agreement and replaces the Provider's previous Data Processing Addendum.

2.3 In the case of conflict or ambiguity between:

(a) any provision contained in the body of this Addendum and any provision contained in Schedules A and B, the provisions in the body of this Addendum will prevail;

(b) any of the provisions of this Addendum and the provisions of the Agreement, the provisions of this Addendum will prevail;

(c) any of the provisions of this Addendum and any completed SCC the provisions of the SCC will prevail.

2.4 The obligations contained in this Addendum shall apply to any Affiliate of the Provider who processes data under the Agreement.

3. DATA PROTECTION

3.1 Both parties will comply with all applicable requirements of the Data Protection Legislation in performing their duties or exercising their rights under the Agreement and this Addendum. This Addendum is in addition to, and does not relieve, remove or replace, a party's obligations under the Data Protection Legislation.

3.2 The parties acknowledge that for the purposes of the Data Protection Legislation, in respect of any personal data that is processed by the Provider on behalf of the Client in the course of providing the Services, the Client is the controller and the Provider is the processor (where Controller and Processor have the meanings given to them in the Data Protection Legislation). Schedule 1 sets out the scope, nature and purpose of processing by the Provider, the duration of the processing and the types of Personal Data and categories of Data Subject.

3.3 Without prejudice to the generality of clause 3.1, the Client will ensure that it has all necessary appropriate consents and notices in place to enable lawful transfer of the Personal Data to the Provider for the duration and purposes of this data processing agreement.

3.4 Without prejudice to the generality of clause 3.1 the Provider shall, in relation to any Personal Data processed in connection with the performance by the Provider of its obligations under this agreement:

(a) process that Personal Data only on the written instructions of the Client unless the Provider is required by Applicable Laws to otherwise process that Personal Data. The Client's instructions shall be contained in or be given in accordance with the Agreement;

(b) where the Provider is relying on laws of a member state of the European Union or the law of the European Union as the basis for processing Personal Data, promptly notify the Client of this before performing the processing required by the Applicable Laws unless those Applicable Laws prohibit the Provider from so notifying the Client;

(c) take all reasonable steps to ensure the reliability of all personnel who have access to and/or process Personal Data and shall ensure that all such personnel are obliged to keep the Personal Data confidential and that access to Personal Data is limited to those individuals who need to have access to Personal Data for the purposes of the agreement and to comply with Applicable Laws;

(d) ensure that it has in place appropriate technical and organisational measures to protect against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data, appropriate to the harm that might result from the unauthorised 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 (those measures may include, where appropriate, pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of its systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the technical and organisational measures adopted by it);

(e) not enter into any Restricted Transfer unless the following conditions are fulfilled:

(i) the transfer is made to an adequate country or the Provider has provided appropriate safeguards within the meaning of Data Protection Legislation;

(ii) the Data Subject has enforceable rights and effective legal remedies;

(iii) the Provider complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred;

(f) comply with reasonable instructions notified to it in advance by the Client with respect to the processing of the Personal Data;

(g) assist the Client, at the Client 's cost (save where such assistance is required as a result of a breach by the Provider of its obligations under this Addendum and/or the Agreement in which case such costs will be borne by the Provider) in responding to any request from a Data Subject and in ensuring compliance with its obligations under the Data Protection Legislation with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators;

(h) notify the Client without undue delay on becoming aware of a Personal Data breach and provide the Client with all information listed in article 33 GDPR in its possession, if necessary in phases;

(i) reasonably co-operate with the Client in the Client's handling of a Personal Data Breach, taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Personal Data Breach;

(j) at the written direction of the Client, delete or return Personal Data and copies thereof to the Client on termination of the Agreement unless required by Applicable Law to store the Personal Data.

3.5 The Provider shall maintain complete and accurate records and information (**Records**) to demonstrate its compliance with this Addendum and will allow the Client by its own personnel or by an independent auditor, who shall enter into a confidentiality agreement with the Client, to access to all such Records during the term of the Agreement and for six months after termination provided:

(a) any such access for the purposes of auditing or otherwise inspecting the Records shall be on not less than fourteen (14) days written notice at any time during normal business hours and not more than once during any twelve (12) month period unless:

(i) the Client has reasonable grounds to suspect that a Personal Data breach has occurred; or

(ii) the Client is required or requested to carry out an audit by Data Protection Legislation or a regulatory authority responsible for the enforcement of Data Protection Legislation in any country;

(b) the Client shall make (and shall ensure that any independent auditor makes) reasonable endeavours to avoid causing any damage, injury or disruption to the Provider's premises, equipment, personnel and business during the audit;

(c) the Client shall submit a detailed audit plan to the Provider upon giving notice of an audit, setting out details of the proposed scope and duration of the audit, such audit plan to be agreed between the parties (acting reasonably);

(d) if the scope of the requested audit has been addressed in an audit carried out by a recognised independent third party auditor within twelve (12) months of the Client's request, and the Provider provides written confirmation that there have been no material changes in the controls and systems to be audited, the Client agrees to accept that audit report in lieu of carrying out its own audit;

(e) all audit costs will be borne by the Client, including the reasonable costs of the Provider incurred during the audit.

3.6 The Client consents to the Provider appointing third-party processors of Personal Data under this agreement. The Provider confirms that it has entered or (as the case may be) will enter with each third-party processor into a written agreement substantially on that third party's standard terms of business including terms which are substantially similar to those set out in this Addendum. The Client acknowledges that this may involve a Restricted Transfer and consents to the use of the SCC or another mechanism offering an adequate level of protection in respect of any such Restricted Transfer. As between the Client and the Provider, the Provider shall remain fully liable for all acts or omissions of any third-party processor appointed by it pursuant to this clause 3.6. A list of third-party processors currently used by the Provider is set out in Schedule 2 to this Addendum. The Provider shall provide reasonable prior notice to the Client prior to amending this list.

3.7 Upon either party's reasonable request and at any time during the term of this Addendum and for the purposes of transfers of Personal Data under this Addendum, the parties shall enter into additional trans-border data flow agreements as may be required under applicable Data Protection Legislation, and to maintain such additional trans-border data flow agreement (with any updates and amendments as may be required to reflect changes in the applicable Data Protection Legislation in the SCC and/or in any other transfer mechanism required under the applicable Data Protection Legislation) for the entire period during which Personal Data is processed by the Provider hereunder.

SCHEDULE 1

1. Processing by the Processor

1.1 Scope, nature and purpose of processing

Scope, Nature and Purpose of processing	The Provider will process Personal Data as necessary to provide the Services to the Client and comply with its obligations under the Agreement.
Types of personal data	Identity Data: First name, last name, title, job title, employer Contact and Location Data: home address, work address, email addresses, telephone numbers, IP address (for technical and security reasons) Transaction Data: purchase history, offers made, offers received Interests Data: art collection, collecting interests, art for sale or to sell.
Categories of data subject	Data Controller's employees, agents, advisors and freelancers, including Data Controller's authorised users of the Services Data Controller's customers, prospects, professional contacts and suppliers. Data Controller's website visitors, mailing list subscribers Employees, agents and freelancers of Data Controller's customers, prospects, professional contacts and suppliers

1.2 Duration of the processing

The duration of the processing corresponds to the duration of the Agreement.

SCHEDULE 2

List of third party processors

As per information available at this URL: https://artlogic.net/sub-processors/

SCHEDULE 3 - 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

The Client of Artlogic accepting the Clauses (the **Data Exporter**)

And

Artlogic Media Limited (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 A.

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 (1);

(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 its behalf after the transfer in accordance with its 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 sub-processor** means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor 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 its 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.

2. Details of the transfer

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

3. Third-party beneficiary clause

The data subject can enforce against the data exporter this clause 3, clause 4(b) to clause 4(i), clause 5(a) to clause 5(e) and clause 5(g) to clause 5(j), clause 6.1 and clause 6.2, clause 7, clause 8.2 and clause 9 to clause 12 as third-party beneficiary.

The data subject can enforce against the data importer this clause, clause 5(a) to clause 5(e) and clause 5(g), clause 6, clause 7, clause 8.2 and clause 9 to clause 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.

3.1 The data subject can enforce against the sub-processor this clause 3.1, clause 5(a) to clause 5(e) and clause 5(g), clause 6, clause 7, clause 8.2, and clause 9 to clause 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 sub-processor shall be limited to its own processing operations under the Clauses.

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.

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 Annex B 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 sub-processor 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 Annex B and a summary description of the security measures, as well as a copy of any contract for sub-processing 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 sub-processing, the processing activity is carried out in accordance with clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subjects as the data importer under the Clauses; and

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

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 Annex B 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 sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Annex B 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 sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with clause 11; and

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

6. Liability

6.1 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 sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

6.2 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 its sub-processor 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 or 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 sub-processor of its obligations in order to avoid its own liabilities.

6.3 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 sub-processor 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 sub-processor agrees that the data subject may issue a claim against the data sub-processor 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 sub-processor shall be limited to its own processing operations under the Clauses.

7. Mediation and jurisdiction

7.1 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.

7.2 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.

8. Cooperation with supervisory authorities

8.1 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.

8.2 The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, 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.

8.3 The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in clause 5(b).

9. Governing Law

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

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 Clauses.

11. Sub-processing

11.1 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 sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor 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 sub-processor's obligations under such agreement.

11.2 The prior written contract between the data importer and the sub-processor 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 sub-processor shall be limited to its own processing operations under the Clauses.

11.3 The provisions relating to data protection aspects for sub-processing 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.

11.4 The data exporter shall keep a list of sub-processing 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.

12. Obligation after the termination of personal data processing services

12.1 The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor 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.

12.2 The data importer and the sub-processor 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.

Annex A to the Standard Contractual Clauses

This Annex forms part of the Clauses

Data Exporter

The Data Exporter is the Client of the Provider that is a party to the Clauses.

Data Importer

The Data Importer is Artlogic Media Limited.is a provider of on-line solutions of the art world which processes personal data upon the instruction of the Data Exporter in accordance with the terms of an agreement for the provision of its services to the Data Exporter (the Agreement)

Data Subjects

Data subjects are individuals about whom personal data is provided to the Data Importer via its services under the Agreement by (or at the direction of) the Data Exporter.

Categories of data

The personal data transferred concern the following categories of data: Data relating to individuals provided to the Data Importer via the services under the Agreement by (or at the direction of) Data Exporter.

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data: Data relating to individuals provided to the Data Importer via the services under the Agreement by (or at the direction of) Data Exporter and may include information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Processing operations

The objective of Processing of Personal Data by the Data Importer is the performance of the services pursuant to the Agreement.

ANNEX B to the Standard Contractual Clauses

Annex B forms part of the Clauses.

Description of the technical and organisational security measures implemented by the data importer in accordance with clause 4(d) and clause 5(c) (or documents/legislation attached). The Data Importer currently abides by the security standards in this Annex B. The Data Importer may update or modify these security standards from time to time provided such updates and modifications will not result in a degradation of the overall security of the Services during the term of the Services Agreement.

1. Technical

(a) Servers

Infrastructure

The Data Importer commissions and maintains infrastructure commissioned from Subprocessors who maintain datacentres secured in line with best industry standard practices. These Subprocessors, listed at https://artlogic.net/sub-processors/ maintain good physical security of their datacentres in line with their respective contractual clauses 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.

Server Operating Systems

All servers containing customer data are snapshotted and backed up to ensure redundancy and security. The Data Importer performs regular patching of production server operating systems.

Application Security

The Data Importer develops its applications and products to be secure by design. Secure development practices and code review are employed to minimise the risk of downtime and maximise security. Security testing and scanning is performed on systems both internally and in collaboration with reputable external consultancies.

Businesses Continuity

The Data Importer replicates data over multiple systems to help to protect against accidental destruction or loss. The Data Importer has designed and regularly reviews its business continuity planning/disaster recovery programs. This includes planning for a catastrophic failure on part of one or more of our Subprocessors'.

(b) Networks and Transmission

Data Transmission

Main serving infrastructure network is provided and appropriately secured by the relevant Subprocessors and, where relevant, by the Data Importer itself. The Data Importer transfers data via Internet standard protocols with encrypted connections and their individual workstations connect to the Internet either via a private link and / or is secured by a VPN employing industry standard secure protocols.

External Attack Surface

The Data Importer maintains minimal footprint in terms of external attack surface in regards to the networks maintained by themselves with relevant Subprocessors guaranteeing the same for networks they maintain. All networks employ a firewall configured to allow only the required connections and the configuration is regularly reviewed and updated in line with best security practice and business requirements.

Incident Detection

Incident detection is intended to provide insight into ongoing incidents and provide adequate information to respond to events affecting uptime and security. The Data Importer incident detection involves preventative measures to reduce scope for failures and attack surface, logging and detection at certain entry-points (e.g. login mechanisms) and employing automated mechanisms that remedy a range of incidents without human interaction.

Incident Response

The Data Importer monitors a variety of communication channels for security incidents, and The Data Importer's server operations personnel will react promptly to known incidents.

Encryption Technologies

The Data Importer makes HTTPS encryption (also referred to as SSL or TLS connection) available by default wherever possible, employing configuration in line with current security standards and business requirements. Data is encrypted at rest and another layer of encryption is applied to particularly sensitive data.

2. Access control.

Access to our systems, our network and our premises and all our devices and servers is heavily restricted. Nearly all Client Data is stored and processed in Cloud-based environments.

3. Data.

(a) Data Storage, Isolation and Logging

The Data Importer stores data in a multi-tenant environment on the servers commissioned by the Data Importer from relevant Subprocessors. The data is backed up in several geographic locations. The Data Importer logically isolates the Data Exporter's data. The Data Exporter will be given control over specific mechanisms for sharing personal data in order to provide the Services. Extensive logging is in place and, where relevant, made available to the Data Exporter for purposes of maintaining and enforcing policies internally.

(b) Decommissioned Media and Media Erase Policy

Any physical devices on the Data Importer's own premises, containing client-supplied data, are returned to the client, and / or securely erased. Data storage on our own devices is securely erased and / or physically destroyed. All devices are encrypted and can be remotely erased.

4. Personnel Security.

The Data Importer personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. The Data Importer conducts reasonably appropriate background checks to the extent legally permissible and in accordance with applicable local employment law and statutory regulations.

Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, the Data Importer's security training, data handling and privacy data training.

Personnel handling customer data are required to complete additional training appropriate to their role. The Data Importer's personnel will not process customer data without authorization. Access to customer data is only permitted to trained personnel under supervision. Access is logged and permissions are granted on the basis of need within someone's role.

5. Subprocessor Security

Before onboarding Subprocessors, the Data Importer carefully reviews the security and privacy practices of Subprocessors to ensure Subprocessors provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once the Data Importer has assessed the risks presented by the Subprocessor, the Subprocessor enters an agreement providing appropriate security, confidentiality and privacy contract terms.

6. Our Data Protection Team

The Data Importer's Cloud Data Protection Team can be contacted at https://artlogic.net/data-protection/ (and/or via such other means as Artlogic may provide from time to time).