DATA PROCESSING AGREEMENT

TRUSTMOORE

This Data Processing Agreement ("DPA") reflects the requirements of:

1. The General Data Protection Regulation ("GDPR") where Trustmoore processes personal data on behalf of a client located within the EEA;
2. UK General Data Protection Regulation and the Data Protection Act 2018, it applies where Trustmoore processes personal data on behalf of a client located in the United Kingdom;
3. The Swiss Federal Act on Data Protection (revFADP), where Trustmoore processes personal data on behalf of a client located in Switzerland.
4. The Singapore Personal Data Protection Act 2012 (PDPA) where Trustmoore processes personal data on behalf of a client located in Singapore.
5. Curaçao Data Protection legislation, including the Landsverordening Bescherming Persoonsgegevens (LBP) and related supervisory guidelines where Trustmoore processes personal data on behalf of a client located in Curaçao or subject to Curaçao data protection laws;

As it applies to the relationship between Trustmoore Group and its clients with regard the processing of personal data.

This DPA forms part of all service agreements between any Client and any entity of the Trustmoore Group. This DPA applies where a Trustmoore Group entity processes Personal Data on behalf of a Client in the capacity of a Data Processor, in connection with services rendered under the relevant services agreement.

However, the DPA does not apply in instances where the relevant Trustmoore entity provides trust, directorship or domiciliation, or a combination of these with other services, insofar as such activities require the Trustmoore entity to process Personal Data for its own purposes and in accordance with its own legal and regulatory obligations (including compliance with anti-money laundering, tax, accounting, and corporate governance rules). In such cases, the Trustmoore entity shall act as an independent Data Controller, and the processing of Personal Data shall be subject to the Trustmoore Group's applicable privacy policies, available at: https://trustmoore.com/data-privacy-policy/, rather than this DPA.

By entering into a Services agreement or using Trustmoore's services, the Client agrees to and accepts the terms of this DPA, unless otherwise agreed in writing. This DPA is incorporated by reference into all applicable agreements with Trustmoore Group entities.

In this Agreement, when written with a capital, the following words and phrases shall have the following meaning, unless otherwise can be derived from the context:

Agreement	:	This Data Processing Agreement and all its Annexes and Schedules
Appendix	:	An appendix with this Agreement
Cessation Date	:	The date on which the Data Controller ceases to share Personal Data with the Data Processor following the termination of the SA

DATA PROCESSING AGREEMENT

TRUSTMOORE

Client		Entity (including object company) receiving services from any Trustmoore group entity, where Trustmoore processes personal data on behalf of that entity
Client Personal Data	:	Any Personal Data Processed by the Processor or a Subprocessor on behalf of the Client pursuant to or in connection with the SA
Data Controller		The Client when acting as Controller
Data Processor	:	Trustmoore when acting as a Processor
Data Protection Laws	:	All applicable laws and regulations relating to the processing of Personal Data and privacy, including without limitation: • The General Data Protection Regulation (EU) 2016/679 (GDPR); • The UK General Data Protection Regulation and the UK Data Protection Act 2018; • The Landsverordening Bescherming Persoonsgegevens (LBP) and any applicable supervisory guidance in Curaçao; • The Personal Data Protection Act 2012 (PDPA) of Singapore; • The Swiss Federal Act on Data Protection (as revised, "revFADP"); • Any other applicable local or international laws, regulations, or binding guidance relating to data protection, privacy, or the processing of Personal Data, including laws governing data security and breach notification;
Data Transfer	:	A transfer of Client Personal Data from the Client to a Processor; or an onward transfer of Client Personal Data from a Processor to a Subprocessor, or between two establishments of the Processor, in each case, where such transfer would not be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws)
EEA	:	European Economic Area

DATA PROCESSING AGREEMENT

TRUSTMOORE

GDPR	:	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (GDPR) for the transfer of Personal Data to a third country
Information Security Policy	:	Trustmoore's internal policy governing the appropriate security measures and procedures implemented for safeguarding personal data processed by Trustmoore
SA	:	The services agreement as entered into by Trustmoore and Client (or object company)
Processing	:	Processing includes the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination**,** restriction, erasure or destruction of personal data. The GDPR applies to the processing of personal data wholly or partly by automated means as well as to non-automated processing, if it is part of a structured filing system.
Schedule	:	A schedule with this Agreement
Services	:	The services the Client provides as described in the respective article of the SA
Subprocessor	:	Any person or legal entity appointed by or on behalf of Processor to process Personal Data on behalf of the Client in connection with the Agreement.
Third-party Claim	:	A claim for compensation by a third party in connection with the Processing of Personal Data.
TMG Data Privacy Policy	:	Trustmoore's Privacy Policy which can be found here: https://trustmoore.com/data-privacy-policy/ as amended from time to time
Trustmoore		Trustmoore Group and all of its directly or indirectly controlled subsidiaries and affiliates globally, as listed Annex 1 to the TMG Data Privacy Policy which can be found here: https://trustmoore.com/data-privacy-policy/

DATA PROCESSING AGREEMENT

TRUSTMOORE

The terms, "Commission", "Controller", "Processor", "Data Subject", "Member State", "Personal Data", "Personal Data Breach", "Processing" and "Supervisory Authority" shall have the meanings assigned to them under the applicable Data protection laws, and their cognate terms shall be construed accordingly. Where terms differ slightly between these laws, their cognate terms shall be construed accordingly based on the governing jurisdiction of the Client relationship.

Article 1. *Purpose of Processing of Personal Data*

1. The Data Processor may process Personal Data on behalf of the Client when rendering the Services under the SA.
2. The Data Processor will process Personal Data exclusively on the written instructions of the Data Controller received via email or by any other means agreed between the Parties, in accordance with the processing purposes and with the means as determined by or in cooperation with the Data Controller, unless the Data Processor must act differently pursuant to applicable laws and regulations.
3. If the Client instructs the Data Processor to process Client Personal Data, the Client warrants the (monitoring of) correctness, completeness and lawfulness of the acquisition and processing of the Personal Data.
4. The details of the Processing, and in particular the categories of Personal Data that are processed and the purpose(s) for which they are processed, are specified in Annex I.
5. The Data Processor shall:
   a. comply with all applicable Data Protection Laws in the Processing of Client Personal Data; and
   b. not Process Client Personal Data other than on the relevant Client's documented instructions.

Article 2. *Term and Effect*

1. This Agreement enters into force as of the effective date stated in the respective SA.
2. This Agreement shall be terminated upon the date of the termination of the SA without any notice being due.
3. Notwithstanding paragraph 2 of this article, this Agreement shall remain in force after the termination of the SA, if and for as long as the Data Controller provides Personal Data to the Data Processor.
4. Subject to the termination of the SA, at the Client's discretion, the Data Processor may: (i) delete/erase or (ii) return to the Client (whether or not by way of a back-up file) the Personal Data and files received within reasonable period of time, unless retention or storage is necessary for the Processor pursuant to a statutory/regulatory obligation.
5. The Data Processor shall provide written certification to the Client that it has fully complied with Article 2.4 within reasonable period of time after the Cessation Date.

Article 3. *Liability*

1. In the context of this Agreement, any liability of the Data Processor to the Data Controller shall be limited at all times to three times the amount of the fee invoiced by the Data Processor during the last calendar year pursuant to the SA, subject to a maximum of €100,000 (in words: one hundred thousand euros), except in so far as there has been:
   a. An intentional act or omission or gross negligence on the part of the Data Processor;
   b. A violation proved by the Client of an obligation to which the Data Processor is specifically subject under the Data Protection Legislation, and
   c. Actions by the Data Processor in conflict with the lawful instructions of the Data Controller.

2. Liability of the Data Processor for any consequential loss, including (but not limited to) lost profits, missed income and reputational damage, shall always be excluded.

Article 4. *Third-party Claim*

1. In case a third party (including: a Data Subject) submits a Third-party Claim to the Data Processor, the Data Processor must inform the Data Controller of this immediately and allow full inspection of the facts and documents known to it.
2. In its defense against the Third-party Claim, the Data Controller must always consider the reasonable and legitimate interests of the Data Processor and inform the Data Processor of each procedural action and consult with it about the strategy to be followed. Both the Data Controller and Data Processor may only agree to an arrangement, settlement, judgment or other measure relating to a Third-party Claim after prior written consultation with the other Party.

Article 5. *Processor Personnel*

1. The Data Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Subprocessor who may have access to the Client Personal Data.
2. The Data Processor will ensure that access to the Client Personal Data is strictly limited to those individuals who need to know / access the relevant Client Personal Data, as strictly necessary for the purposes of the SA, and to comply with Applicable Laws in the context of that individual's duties to the Processor.
3. The Data Processor will ensure that all such individuals and entities are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

Article 6. *Security*

1. The Data Processor shall in relation to the Client Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.
2. In assessing the appropriate level of security, the Data Processor shall take into account the particular risks that arise from the Processing of the Client Personal Data, in particular the risk and impact of a Personal Data Breach.

Article 7. *Subprocessing*

1. The Data Processor is allowed to appoint another entity within the Data Processor's group of entities as a Subprocessor under this Agreement.
2. The Data Processor shall not appoint (or disclose any Client Personal Data to) any other Subprocessor outside the Data Processor's group of entities unless such Subprocessor applies at least the same level of data safeguarding measuers as the Data Processor.

Article 7a. Intragroup Data Sharing

1. The Data Processor may disclose or make available Client Personal Data to other entities within the Trustmoore Group, provided that such disclosure is:
   - necessary for the performance of the Services under the SA;
   - required for internal administrative purposes, including group-level risk management, compliance, multijurisdictional Client onboarding or servicing, or IT support;

- based on a legitimate interest of the Trustmoore Group that does not override the interests or fundamental rights and freedoms of the Data Subjects.

2. In all such cases, the Data Processor shall ensure that the recipient Trustmoore Group entity:
   - is subject to appropriate confidentiality and data protection obligations consistent with this Agreement;
   - complies with applicable Data Protection Laws; and
   - processes the Client Personal Data solely for the purposes outlined above.
3. Transfers of Client Personal Data outside the Client's jurisdiction, where applicable, shall be subject to Article 12 (Data Transfer) of this Agreement.

Article 8. *Data Subject Rights*

1. The Data Processor shall support the Data Controller with implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the obligations of the Data Controller under the Data Protection Laws with regard to Data Subject rights.
2. The Data Processor shall:
   - promptly notify Data Controller if it receives a request from a Data Subject under any Data Protection Law in respect of Client Personal Data; and
   - ensure that it does not respond to that request except on the written instructions of the Client or as required by applicable laws to which the Data Processor is subject, in which case the Data Processor shall to the extent permitted by applicable laws inform Client of that legal requirement before the Processor responds to the request.

Article 9. *Personal Data Breach*

1. The Data Processor shall notify the Data Controller without undue delay, but in any case not later than 24 hours, upon the Data Processor becoming aware of a Personal Data Breach affecting Client Personal Data. The Data Processor will provide the Client with sufficient information to enable the Client to meet any reporting obligations or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.
2. The Data Processor shall cooperate with the Client and take reasonable steps as are directed by the Client to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

Article 10. *Data Protection Impact Assessment and Previous Consultation*

The Data Processor shall provide reasonable assistance to the Data Controller with data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Client reasonably considers to be required under article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Client Personal Data, and taking into account the nature of the Processing and information available to the Processor.

Article 11. *Audits rights*

1. Subject to this article, the Data Processor shall make available to the Data Controller on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by the Data Controller or an auditor mandated by the Data Controller, in relation to the Processing of the Client Personal Data by the Data Processor.

2. The previous Section 11.1 will be applicable to the extent that the SA, or other agreements between the Data Controllse and the Data Processor, do not already cover such rights meeting the requirements of the Data Protection Laws.

Article 12. *Data Transfer*

1. The Data Processor shall not transfer or permit the transfer of Client Personal Data to a country or territory outside of the Client's jurisdiction (and, where applicable, outside of the EEA, UK, or Switzerland) unless it ensures that such transfer complies with applicable Data Protection Laws.
   - In cases where such transfers occur, the Data Controller and the Data Processor agree that appropriate safeguards shall be implemented, including, where required:
   - the use of EU Standard Contractual Clauses adopted by the European Commission (including any applicable Modules under Commission Implementing Decision (EU) 2021/914),
   - the UK Addendum or International Data Transfer Agreement (IDTA) approved by the UK Information Commissioner's Office,
   - or contractual clauses or binding corporate rules recognized by the data protection authority of the relevant jurisdiction (e.g., revFADP in Switzerland or PDPA in Singapore).

2. The Data Controller and the Data Processor further agree to execute any supplementary documentation or assessments (e.g., transfer impact assessments) reasonably necessary to ensure ongoing compliance with Data Protection Laws.
3. If required by applicable law, a separate signed copy of the applicable Standard Contractual Clauses may be requested by the Client and shall be provided by the Data Processor.

Article 13. *Trustmoore acting as Controller*

Following article 2, upon termination of this Agreement Trustmoore may store Personal Data based on Trustmoore's legitimate interest in case of legal claims or ongoing litigation. In all such instances the TMG Privacy Policy will apply.

Article 14. *Confidentiality*

The Data Processor must observe the confidentiality towards third parties of the Personal Data in its possession in the context of this Agreement, unless an applicable statutory provision, code of conduct or professional code, or court order requires it to disclose them, or if this necessarily follows rendering the Services under the SA.

Article 15. *Notices*

1. All notices and communications given under this Agreement must be in writing and will be delivered personally, sent by post or sent by email to the address or email address set out in the SA or at such other address as notified from time to time by the Parties changing address.
2. Any communication or queries regarding this DPA can be addressed to the Data Protection Officer at **privacy@trustmoore.com**.

Article 16. *Partial invalidity, continuing obligations*

1. If one or more articles of this Agreement were to be null and void or non-binding in another way, this does not affect the validity of the other articles of this Agreement, unless the non-binding provisions regard the essence of the Agreement and the other provisions not being affected raise such objections with one of the Parties that reasonableness and fairness order the other articles to be non-binding as well. In both cases Parties will then in

mutual consultation and in the spirit of this Agreement amend this Agreement to the extent necessary, in the sense that the non-binding articles will be replaced by articles that will differ as little as possible from the related non-binding articles.

2. Obligations that by their nature are destined to also continue after termination, continue to exist after termination of this Agreement.

Article 17. *Remedies*

1. Failure to execute, or a delay in the execution, of a right or remedy arising from the underlying Agreement or the law, will not impair the execution of this right or remedy or another right and/or remedy in any way whatsoever.
2. Partial execution of a right, or remedy arising from this Agreement or the law, as yet does not obstruct fully executing this right or remedy, or of the execution of another right or remedy.
3. The rights and remedies arising from the underlying Agreement are complementary and do not exclude any rights or remedies arising from the law.

Article 18. *Applicable law, regulation on disputes*

1. This Agreement shall be governed by the laws of the same jurisdiction as under the SA.
2. Any dispute arising from this Agreement shall be resolved as agreed under the SA.
3. Any dispute arising out of or in connection with this Agreement shall be resolved in accordance with the dispute resolution provisions of the applicable SA. Where no such provisions exist, the Parties agree to submit to the exclusive jurisdiction of the competent courts in the jurisdiction governing the applicable SA.

Article 19. *Miscellaneous*

1. This Agreement can solely be amended or supplemented by means of a document signed by both the Data Controller and the Data Processor.
2. All communication pursuant to this Agreement shall be delivered to the addresses mentioned in the heading of this Agreement, or such other address as may be communicated by one party to the other party, by (registered) mail or courier.
3. None of the rights and/or obligations under this Agreement shall be assignable by a party without the prior written consent of the other parties.
4. The preamble is an integral part of this Agreement.
5. Titles of articles in this Agreement are there purely for identification purposes, and no rights can be derived from them.
6. References to enactments are to such enactments as are from time to time modified, re-enacted or consolidated.
7. Words importing the singular shall include the plural and vice versa and those importing the masculine gender shall include the feminine and the neutral and vice versa in each case.
8. References to clauses and schedules are to clauses and schedules of this Agreement.
9. Words importing persons include companies or associations or bodies of persons whether corporate or unincorporated.

APENDIX I

ANNEX I

B. DESCRIPTION OF THE PROCESSING

I. Categories of Data Subjects whose personal data is processed:

Given the ongoing business relation between the Controller and Processor under the SA, the categories of data subjects may vary, but will at least include the following:

Client employees
Contractors and Suppliers
Directors of the Client and Client Affiliate entities
Client Ultimate beneficial owners
Investors
Trustees
Clients
Contact persons and Ambassadors
Other: as the specific case might require or as per specific instructions by the Data Controller

II. Categories of personal data processed:

General Personal Data: including, but not limited to: First, middle, last name and aliases, business contact information (Client, email, phone, physical business address), personal contact information (email, cell phone, personal address), title, position, employer, copy of passport/ID document, signature, bank account details and information regarding balances, financial information, such as incoming and outgoing payments, payment related documents, user account details, other: as the specific case or as per specific instructions by the Data Controller.

III. Nature and purpose(s) of the data processing:

3.1. Nature of processing: The processing will involve collection, recording, duplication, organisation, structuring, storage, adaptation or alteration, retrieval, disclosure by transmission or otherwise to the extent permitted by law, alignment and combination, erasure or if necessary destruction of the personal data.

3.2.Purposes of processing:

Performance of the services assigned with the SA.

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

The data shall be retained only for the period of time needed to fulfill the purpose of the data processed and as stipulated in the Client's retention policies. Trustmoore will hold the data as stipulated in Art. 2 and Art. 13 of the Agreement.

Technical And Organisational Measures Including Technical And Organisational Measures To Ensure The Security Of The Data:

- Trustmoore adheres to its Information Security Policy; Data Privacy Policy; Retention Policy; Personal Data Breach Procedure and DPIAs;
- Usage and maintenance of devices and security of information and devices during use and storage: All equipment (fixed and mobile) is set up, used and maintained in accordance with the manufacturer's

instructions. No external devices are allowed. The IT staff of Trustmoore ensures that software updates regarding device and software security will be installed on all devices used for the storage or access to personal data as quickly as possible.

- Technical measures: For ensuring technical compliance hereunder the following technical measures are used: data in transit and data at rest is encrypted via encryption tools; all devices are equipped with desktop and laptop firewalls; all devices are equipped with anti-virus and anti-malware software; multifactor authentication approaches are implemented; automated patching and security vulnerability assessments are done regularly; strong physical, environmental, network and perimeter controls are maintained; intrusion, detection and prevention technologies are implemented; monitoring and detection systems are implemented; backup facilities are available;
- Employees only have access to those parts of the buildings of the organization that are for general use or to which access to them by means of a key or access card is granted. Visitors are not allowed in those parts of Trustmoore's buildings where sensitive information is stored or accessible;
- Employees receive periodic trainings on the above policies;