Data Processing Addendum based on EU Standard Contractual Clauses

Commission Implementing Decision (EU) 2021/915 of 4 June 2021

This Data Processing Addendum ("**Addendum**") will apply from **1 August 2021** and will be deemed to be incorporated into all agreements and contracts pursuant to which affiliates and subsidiaries of the Maples Group that are domiciled in the UK, the Channel Islands, or the EU provide their services by acting as a 'processor' as defined in Article 4(8) of GDPR. This Addendum is based on the Commission Implementing Decision (EU) 2021/915 of 4 June 2021, and it automatically supersedes the previous version of the Addendum which applied from 25 May 2018.

Services which Maples provides by acting as a 'processor' include (without limitation) entity formation/registration services, corporate administration and secretarial services, registered office services, fund administration (accounting/NAV calculation service and investor service), and other like services where the role performed by Maples can be characterised as an outsourced function which Maples fulfils by exercising relatively little autonomy or discretion.

For the avoidance of doubt, this Addendum will not apply where Maples acts as a 'controller' (as defined in Article 4(7) of GDPR) in providing the service. Examples of services which Maples provides by acting as a 'controller' include (without limitation) legal services, fund management services, compliance/MLRO services, director/trustee services, and other like services where the role performed by Maples requires Maples to exercise a good degree of autonomy and discretion.

Section I: Preliminaries

1 Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the "**Clauses**") is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

(b) The controllers and processors listed in Schedule 1 have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29(3) and (4) of Regulation (EU) 2018/1725.

(c) These Clauses apply to the processing of personal data as specified in Schedule 2.

(d) Schedule 1 to Schedule 3 are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

2 Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

3 Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

4 Hierarchy

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

5 Docking clause

(a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Schedules and signing Schedule 1.

(b) Once the Schedules in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Schedule 1.

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

Section II: Obligations of the Parties

6 Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Schedule 2.

7 Obligations of the Parties

7.1 Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2 Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Schedule 2, unless it receives further instructions from the controller.

7.3 Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Schedule 2.

7.4 Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Schedule 3 to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5 Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("**sensitive data**"), the processor shall apply specific restrictions and/or additional safeguards.

7.6 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

(d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7 Use of sub-processors

(a) The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub- processor to fulfil its contractual obligations.

(e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8 International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

8 Assistance to the controller

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

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions.

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(i) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(ii) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

(iii) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(iv) the obligations in Article 32 of Regulation (EU) 2016/679.

(d) The Parties shall set out in Schedule 3 the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

9 Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 of Regulation (EU) 2016/679 or under Articles 34 and 35 of Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) of Regulation (EU) 2016/679:

(i) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(ii) the likely consequences of the personal data breach;

(iii) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) in complying, pursuant to Article 34 of Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Schedule 3 all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

Section III: Final Provisions

10 Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(i) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(ii) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

(iii) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1(b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

Schedule 1 (List of Parties)

1 Controller(s)

The controller is the legal entity that has contracted with a Maples Group entity which is domiciled in the EU, the Channel Islands, or the UK, and which acts as a processor, as identified in the relevant underlying service agreement.

The controller's accession date is **1 August 2021**, or if later, the date on which the relevant underlying service agreement was concluded.

The signature of the controller on the relevant underlying service agreement will be deemed to be the controller's signature for these Clauses.

The contact details for the controller are separately notified to the processor by the controller.

2 Processor(s)

The processor is the Maples Group entity which is domiciled in the EU, the Channel Islands, or the UK, and which has contracted with the controller to provide services by acting as a processor, as identified in the relevant underlying service agreement. The Maples Group entities which act (or could potentially act) as a processor or sub-processor for the purposes of these Clauses include, without limitation, the following:

(a) **Maples Fiduciary Services (Ireland) Limited**, 32 Molesworth Street, Dublin 2, D02 Y512, Ireland;

(b) **Maples Fund Services (Ireland) Limited**, 32 Molesworth Street, Dublin 2, D02 Y512, Ireland;

(c) **MFD Secretaries Limited**, 32 Molesworth Street, Dublin 2, D02 Y512, Ireland;

(d) **MaplesFS Trustees Ireland Limited**, 32 Molesworth Street, Dublin 2, D02 Y512, Ireland;

(e) **Maples Owner Trustees Ireland Limited**, 32 Molesworth Street, Dublin 2, D02 Y512, Ireland;

(f) **Maples Fiduciary Services (Jersey) Limited**, 2nd Floor The Le Gallais Building, 54 Bath Street, St. Helier, Jersey JE1 1FW, Channel Islands;

(g) **Maples Nominees (Jersey) No. 1 Limited**, 2nd Floor The Le Gallais Building, 54 Bath Street, St. Helier, Jersey JE1 1FW, Channel Islands;

(h) **Maples Nominees (Jersey) No. 2 Limited**, 2nd Floor The Le Gallais Building, 54 Bath Street, St. Helier, Jersey JE1 1FW, Channel Islands;

(i) **Maples Trustees (Jersey) Limited**, 2nd Floor The Le Gallais Building, 54 Bath Street, St. Helier, Jersey JE1 1FW, Channel Islands;

(j) **Maples Company Secretary (Jersey) Limited**, 2nd Floor The Le Gallais Building, 54 Bath Street, St. Helier, Jersey JE1 1FW, Channel Islands;

(k) **MaplesFS (Luxembourg) S.A.**, 6D route de Trèves, Senningerberg, L-2633 Luxembourg;

(l) **Maples Fiduciary Services (Netherlands) B.V.**, Tower A, Level 12, Strawinskylaan 1209, 1077 XX Amsterdam, Netherlands;

(m) **Maples Fiduciary Services (UK) Limited**, 200 Aldersgate Street, London EC1A 4HD, United Kingdom; and

(n) **MaplesFS UK Group Services Limited**, 200 Aldersgate Street, London EC1A 4HD, United Kingdom.

The processor's accession date is **1 August 2021**, or if later, the date on which the relevant underlying service agreement was concluded.

The signature of the processor on the relevant underlying service agreement will be deemed to be the processor's signature for these Clauses.

Queries concerning processing performed by the processor may be emailed to the controller's usual contact person within the Maples Group, or to Maples Group's Risk & Compliance Function by emailing privacy@maples.com.

Schedule 2 (Description of the processing)

This Schedule 2 describes the processing to be performed by the processor on behalf of the controller.

Note: To the extent the processor performs any processing by itself determining the purpose and manner of processing (i.e. the processor acts as a controller in its own right, for example when using personal data to conduct mandatory KYC checks to meet its own compliance obligations or to maintain/develop its relationship with its clients), the details of such processing are out of the scope of these Clauses, and they are separately described in the Client Privacy Notice adopted by the processor, which can be found online at https://maples.com/privacy.

1 Categories of data subjects whose personal data is processed

(a) **Client Business Contacts**. Individuals who are employed or otherwise engaged by the controller or its affiliates/subsidiaries, and who interact with the processor in connection with the provision of the services to the controller by the processor.

(b) **Business Owners**. Individuals who are in control of the controller or its affiliates/subsidiaries by virtue of being the beneficial owners (regardless of the form of ownership), as well as individuals who exercise control over the controller or its affiliates/subsidiaries through executive powers vested in them (regardless of whether or not they hold any ownership interest in the controller or its affiliates/subsidiaries).

(c) **Service Beneficiaries**. Individuals who directly or indirectly benefit from the services provided to the controller by the processor, for example:

(i) directors, officers, and shareholders of the controller or its affiliates/subsidiaries who receive registered office service or board support services from the processor; and

(ii) individuals who invest in investment funds which are set up, sponsored, or promoted by the controller or its affiliates/subsidiaries, and supported by the processor.

(d) **Other Relevant Individuals**. Individuals who do not belong to any of the foregoing categories but nevertheless interact with the processor in connection with (or are otherwise affected by) the services provided by the processor, e.g. other professional advisors and service providers who are separately engaged by the controller.

2 Categories of personal data processed

(a) **Contact Details**. The data subject's contact details such as title, name, postal address, email address, and phone number.

(b) **KYC Records**. Information about the data subject which the controller is obliged to check for legal or regulatory reasons, such as date of birth, country of residence, nationality, ownership interest in entity or asset, source of wealth, tax status, and other like information concerning the data subject's identity and background.

Note: KYC Records will be processed by the processor on behalf of the controller only where the controller instructs the processor to conduct the relevant checks on behalf of the controller (e.g. where investor KYC forms part of the fund administration service the processor provides to the controller).

(c) **Service Records**. Information about the data subject which the processor obtains in order to provide services to the controller. Depending on the circumstances and the nature of with relationship between the data subject and the processor, such information may include, without limitation:

(i) any directorship / partnership held by the data subject;

(ii) opinions expressed and actions taken by or against the data subject in connection with operation of the controller's business;

(iii) investments the data subject makes in (or redeems from) investment funds which the processor administers on behalf of the controller,

(iv) actions the processor take towards the data subject based on instruction received from the controller; and

(v) information about the data subject's education, experience, professional qualification, and personal circumstances.

3 Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures

Whilst the possibility of sensitive data being processed by the processor cannot be ruled out, the parties acknowledge and agree that it is unlikely that sensitive data (i.e. personal data which falls within the ambit of Articles 9 and 10 of Regulation (EU) 2016/679) will need to be processed by the processor on behalf of the controller.

If and to the extent the processor identifies any sensitive data amongst the personal data it processes on behalf of the controller, the processor must ensure that appropriate restrictions which are commensurate with their sensitivity are applied to such sensitive data (especially in relation to access control and other security measures described in Section 1 of Schedule 3).

4 Nature of the processing

The personal data will be subject to collection, use, combination, disclosure, retention, and all other processing operations which are inherent in or necessary to facilitate the provision of services by the processor in accordance with the underlying service agreement.

The processing performed by the processor include recurring or regular processing (e.g. production of minutes of board meetings or investor statements on behalf of the controller), as well as ad hoc or one-off processing (e.g. regulatory filing made in connection with incorporation of legal entities on behalf of the controller).

5 Purpose(s) for which the personal data is processed on behalf of the controller

(a) **Service Delivery**. To facilitate the provision of services to the controller by the processor (which may in turn, directly or indirectly, facilitate the services the controller provides to its customers). The precise description of the services to be provided by the processor is set out in the relevant underlying service agreement between the controller and the processor. A generic description of the services which may be provided to the controller by the processor can be found online at:

(i) https://maples.com/en/services/fund-services;

(ii) https://maples.com/en/services/fiduciary-services; and

(iii) https://maples.com/en/services/entity-formation-and-management-services.

(b) **Legal and Regulatory Compliance**. To enable the controller to comply with all relevant legal and regulatory requirements, including, without limitation, legal requirements relating to money laundering, tax evasion, and sanctions/embargoes.

6 Duration of the processing

The processing will be carried out for as long as the processor is required to provide its services to the controller in accordance with the relevant underlying service agreement. Where the relevant underlying service agreement has expired or is terminated for any reason, the processor will cease the processing on behalf of the controller, save for any processing which is necessary to comply with Clause 10(d).

Schedule 3 (Technical and organisational measures including technical and organisational measures to ensure the security of the data)

This Schedule 3 describes the technical and organisational security measures implemented by the processor(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, as well as the risks for the rights and freedoms of natural persons.

The Maples Group takes information security very seriously and considers it an on-going effort and not a point-in-time project. As a result, the Maples Group is committed to providing robust systems by continually evaluating and implementing enhancements in our security technologies. Underscoring this commitment is our continuous approach to improving our information security offering, which covers three very critical areas — physical, system and operational security — via a dedicated Information Security Practice within the Maples Group.

The Maples Group protects client information using the following measures:

1 Security

Arrangements made to protect system resources from unauthorised access, use, or modification.

(a) Dedicated Information Security Manager focused on enterprise security.

(b) Security awareness including training on information security roles and responsibilities.

(c) Policies and procedures (based upon ISO standards) in place to ensure that employees, contactors and third parties understand their respective roles and responsibilities.

(d) Incident reporting and response process to ensure that incidents are identified, reported, escalated, and tracked through resolution.

(e) Crisis management teams and process established for management during adverse situations

(f) Independent third party reviews of operations and technology.

(g) Firewall architectural design ensures that all external points-of-presence are protected.

(h) Event logs record activities, exceptions, faults and information security events.

(i) Malware scanning of all inbound and outbound email messages and Internet traffic.

(j) Web Application Firewall protects internet facing platforms against web application attacks.

(k) Intrusion detection system monitoring of Internet connection points.

(l) Vulnerability scanning routinely performed to detect security weaknesses.

(m) Physical Security controls ensure that only authorised personnel are allowed access.

(n) Strong authentication to reduce the risk of unauthorised access.

(o) Access control reviews are conducted on a regular basis.

(p) Privileged support accounts are restricted and controlled.

2 Availability

Arrangements made to support system accessibility for operation, monitoring, and maintenance.

(a) Uninterruptible power supplies, generators, redundant power sources, air conditioning units, and fire suppression systems provide support for critical systems to guard against environmental hazards, e.g. fire, dust, power surge/loss, excessive heat, water, and humidity.

(b) Business Continuity (BC) and Disaster Recovery (DR) plans exist for all critical business functions.

(c) BC/DR plans are reviewed annually for adequacy of resources (people, technology, facilities and funding).

(d) BC/DR plans are tested on a regular basis and test results reviewed to identify improvements.

(e) Backup and recovery procedures are documented, implemented and tested.

(f) System Development Life Cycle includes project management of all major deliverables, i.e. business, functional and technical specifications, a documented test plan, and implementation/roll-out plan.

(g) Change control process of production changes are planned scheduled and coordinated.

(h) Testing performed on all major application changes.

(i) Procedures are in place to ensure that software remains current and supported.

(j) Systems are proactively monitored for performance, availability and capacity.

3 Confidentiality

Arrangements made to protect information throughout its life cycle, final disposition and removal from the system.

(a) Confidential data is encrypted while stored (data-at-rest).

(b) Confidential data is encrypted while in-transit on untrusted networks (data-in-transit).

(c) Removable media is controlled and monitored to prevent unauthorised disclosure, modification and removal of confidential information.

(d) Third party service providers must sign confidentiality / non-disclosure agreements before accessing Maples Group systems.

(e) Enterprise data loss prevention (DLP) solutions are implemented, monitored, and maintained.

4 Other measures to assist the controller(s)

Processes, policies, and procedures are in place to ensure that:

(a) requests, queries, and complaints relating to personal data made by the relevant data subjects ("**Data Subject Requests**") as well as personal data breaches are promptly identified and escalated internally to the Maples Group's Risk & Compliance function;

(b) Data Subject Requests and personal data breaches are further escalated as necessary to the relevant controller in accordance with Clause 8 and Clause 9;

(c) all such assistance as the controller may reasonably require to ensure compliance with Regulation (EU) 2016/679 and other applicable privacy laws and regulations are provided in accordance with Clause 8. Such assistance may, if and to the extended warranted in the context, include:

(i) providing copies of the relevant personal data to the controller or any other person specified by the controller;

(ii) correcting any inaccuracy or incompleteness in the relevant personal data;

(iii) deleting, anonymising, or pseudonymising the relevant personal data;

(iv) refraining from processing the relevant personal data in any specific manner as specified by the controller;

(v) assisting the controller in performing the risk assessment of processing carried out by Maples;

(vi) assisting the controller in consulting the relevant authorities in relation to the processing carried out by Maples; and

(vii) communicating with the relevant authorities and the data subjects in the event of a personal data breach;

(d) The controller may contact the Maples Group's information security team by emailing security@maples.com to discuss the information security measures implemented by Maples; and

(e) The controller may contact the Maples Group's Risk & Compliance function by emailing privacy@maples.com to discuss other aspects of the compliance measures implemented by the Maples.