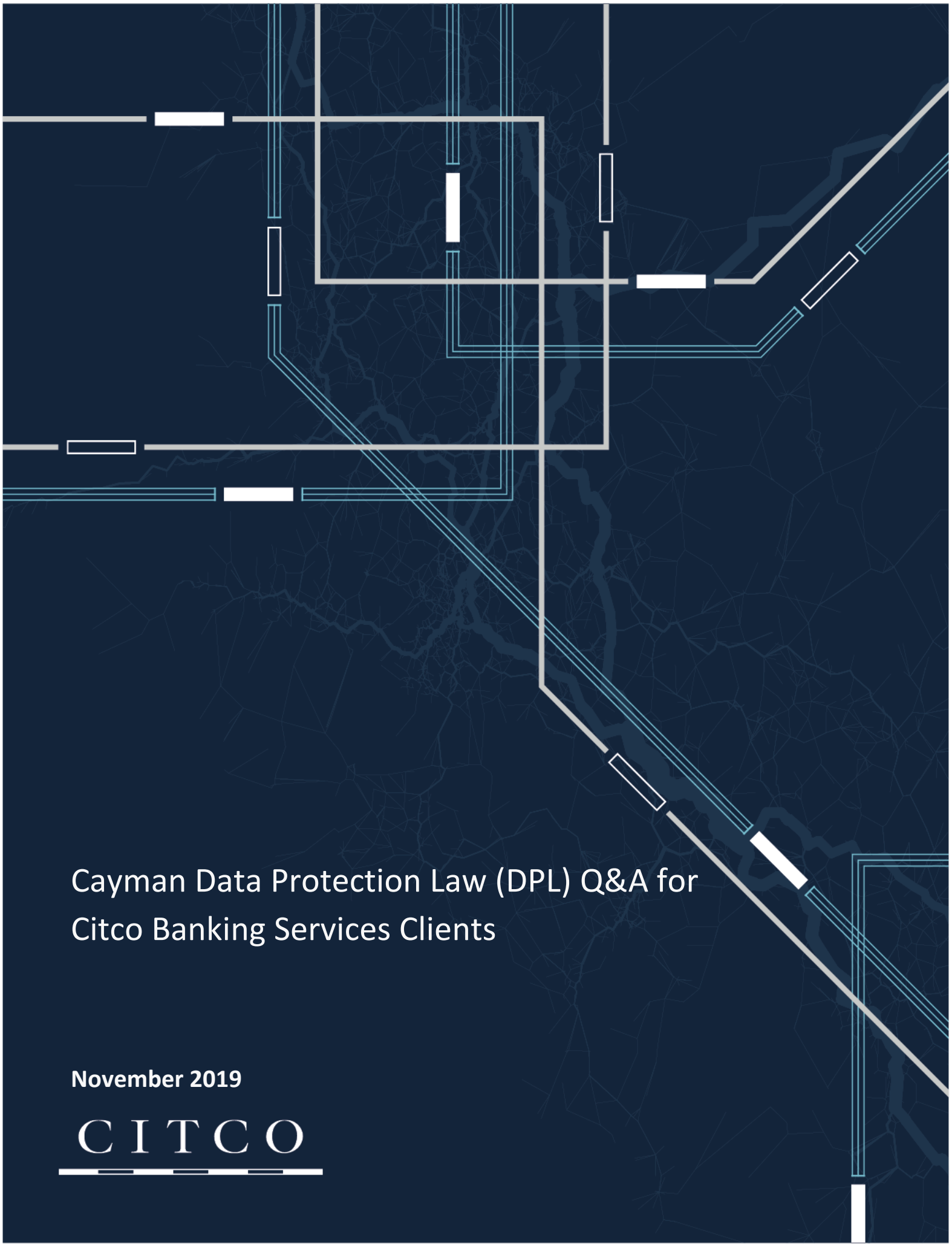

Cayman Data Protection Law (DPL) Q&A for Citco Banking Services Clients

November 2019

CITCO

Table of Contents

I. Overview

On 27 March 2017, the Data Protection Law, 2017 (http://www.gov.ky/portal/pls/portal/docs/1/12428349.PDF) was passed by the Legislative Assembly of the Cayman Islands. Cayman has delayed the introduction of this law until September 30, 2019. (It was originally scheduled to be enforceable since January 2019.)

The Cayman data protection law makes a distinction between data controllers and processors in the same way the European General Data Protection Regulation ("GDPR") does (and the EU's 1995 Data Protection Directive before it). This is because the Cayman DPL is influenced by the 1995 Directive. The definitions of a data "controller" and a data "processor" are effectively the same as the definitions contained in the GDPR. Therefore, references to data controller and data processor roles are relevant irrespective of whether the GDPR or the Cayman DPL (once enforceable) applies to a particular Citco Cayman client entity relationship.

All Cayman funds should take steps to ensure they understand their obligations under the new law. We have prepared this Q&A document to assist you in that regard. In addition, we have prepared a comparison chart between the Cayman DPL and the GDPR. We have also prepared a table showing more specifically how Citco has prepared for the Cayman DPL.

II. Cayman DPL - Q&A

Questions		Response / Comments
1.	Who does the DPL apply to?	The DPL applies to processing of personal data carried out by organizations established within the Cayman Islands, as well as to organizations established outside the Cayman Islands that process personal data within the Cayman Islands. Although the DPL has implications for "data processors", it primarily applies to "data controllers".
2.	What is personal data or sensitive data?	The DPL applies to "personal data" meaning any information relating to a living individual who can be directly or indirectly identified. The DPL applies to personal data in any format, including in automated and manual (paper) filing systems. The DPL refers to "sensitive personal" data, to which additional protections apply. Sensitive personal data includes genetic and health data, as well as information on racial or ethnic origins, political opinions, religious or similar beliefs, sex life, the commission or alleged commission of an offence.
3.	What is a "data processor"?	**Data Processor** A "data processor" processes personal data on behalf of a data controller and does not itself determine why personal data should be processed. However, a data processor may to a certain extent, decide on how the personal data should be processed. As defined by the DPL: - *any person who processes personal data on behalf of a data controller but, for the avoidance of doubt, does not include an employee of the data controller* The DPL does not apply directly to data processors but where data processors are appointed by a data controller (that is subject to the DPL), certain contractual assurances with respect to the processing of personal data are required to be put in place. The data processor does not need to be in the Cayman Islands.

4.	What is a "data controller"?	**Data Controller** A "data controller" exercises control over personal data; they determine why and how personal data is processed. As defined by the DPL: - *the person who, alone or jointly with others determines the purposes, conditions and manner in which any personal data are, or are to be, processed and includes a local representative* You are a data controller if you are: - *established in the Cayman Islands, and the personal data is processed in the context of that establishment; or,* - *not established in the Cayman Islands but the data is being processed in the Cayman Islands (otherwise than for transit purposes).* In all situations, a Cayman fund or client entity is the "data controller". Owing to the nature of banking services (which require the exercise of a considerable degree of discretion and autonomy while handling personal data), Citco Bank and Trust Company Limited ("Citco Cayman") is also a data controller in its own right, albeit that it is a service provider. As a result, a data controller-data processor relationship does not exist and data controller-data processor contract obligations are not relevant. Instead, a data controller-data controller relationship exists. In terms of the form of this relationship, Citco Cayman (as a provider of banking services) determines the purposes and means of processing the personal data separate and independent of the Cayman fund or entity's purposes and means of processing of the personal data. Accordingly, in their respective capacities as data controllers, Citco Cayman and the relevant Cayman fund or client entity are separate (or independent) data controllers. Therefore, a joint controller relationship between Citco Cayman and the entities that it services does not arise. It follows that each data controller is (in its own right) directly subject to the DPL without a direct contractual link. **Where a non-Cayman established separate and independent data controller provides services to a controller that is within the scope of the DPL** In some circumstances, a Cayman fund or client entity may receive data controller services from another Citco entity situated outside of the Cayman Islands (e.g. depositary services that may include custodian services). Given the nature of the services that Citco provides as a depositary, it is a data controller separate to the Cayman fund or client entity (which is also a data controller). A data controller to data processor relationship does not exist. By reason of such services being provided to non-natural persons (i.e. the services are not offered or provided to natural persons, instead, they are offered to, provided to and contracted for with the Cayman fund or client entity), the non-Cayman Citco data controller entity is outside the scope of Section 6(1)(b) of the DPL and DPL data processing terms are not required. As a result, where a non-Cayman Citco entity has reason to process Cayman resident personal data when providing data controller services to a Cayman fund or client entity, its immediate data protection compliance obligation is to the

		relevant data subjects in accordance with the relevant data protection laws that the relevant non-Cayman Citco entity is subject to. Therefore, because non-Cayman Citco entities offering depositary (which may include custodian) services are recognised as separate controllers from the Cayman funds or client entities, they are not subject to the requirements of the Cayman DPL. It is worth noting that if a (very unlikely) joint controller relationship exists (e.g. between a Citco non-Cayman entity and a Cayman fund or client entity), the Ombudsman Guidelines state, "*While not explicitly mentioned in the DPL, it is best practice for joint controllers to enter into a joint controllership agreement, which will lay out the parties' respective responsibilities*." This would naturally impose some form of Cayman DPL obligations on a non-Cayman controller where the other joint controller is established in Cayman (Page 19 of the Cayman Ombudsman Guidelines for Data Controllers, v1.03 January 2019 -https://ombudsman.ky/images/pdf/pol_guide/Data-Protection-Law-2017---Guide-for-Data-Controllers.pdf).
5.	Do I need a "representative"?	Where Citco Cayman services client entities that have been incorporated or established in Cayman, those client entities (subject to some exemptions) would *not* require a Cayman local representative as they would be treated as "established" in Cayman in accordance with Section 6(3). Where the client entity is not incorporated or established in Cayman, but is serviced by Citco Cayman, the client entity must nominate a local representative. *- Section 6(2) of the DPL, a Data Controller "shall nominate, for the purposes of this Law, a local representative established in the Islands who shall, for all purposes within the Islands, be the data controller and, without limiting the generality of this provision, bear all obligations under this Law as if the representative was a data controller."*
6.	What are my contractual obligations as a controller?	A data controller who engages a data processor must ensure that the engagement is based on a written contract, which contains certain prescribed assurances which conforms to the requirements of the DPL regarding the processing of personal data.
7.	What is considered "processing of personal data"?	The DPL defines this broadly. Processing can be defined as: *obtaining, recording or holding data, or carrying out any operation or set of operations on personal data, including -* *(a) organizing, adapting or altering the personal data;* *(b) retrieving, consulting or using the personal data;* *(c) disclosing the personal data by transmission, dissemination or otherwise making it available; or* *(d) aligning, combining, blocking, erasing or destroying the personal data*
8.	What has Citco done to prepare for the DPL?	Citco has put together a comprehensive privacy program in 2016 to oversee the implementation of the GDPR. It took into account Privacy Leadership, Training & Awareness, Compliance with laws and regulations, Security, Incident Response, Policies and Procedures, Privacy by Design and Default, Individual Data Subject Rights, Privacy Controls & Risk Management, and Enforcement & Redress. Because of this, (contractual amendments notwithstanding), we feel we conform to all the requirements of the Cayman DPL. You may visit our privacy page or see the tables below for additional information.

9.	Potential overlap of Cayman DPL with the GDPR	**Where data controller services are provided to Cayman fund and client entities by an EEA established Citco entity** The Citco group of companies applies a GDPR standard of compliance across its organisation. The question of whether GDPR data subject rights are given to an individual depends on whether the relevant Citco entity is subject to Article 3(1) or Article 3(2) of the GDPR. If the Citco entity is outside the scope of the GDPR, GDPR rights are not available to the data subjects that have their personal data processed during the course of the provision of the service to a client entity. As depositary services are typically delivered by Citco entities established in the EEA, these services are within the scope of the GDPR by reason of Article 3(1) irrespective of the location of the client fund or entity. Although the volume of personal data processed as part of this service delivery is minimal, it is still technically necessary to give GDPR rights to all individuals that have their personal data processed as a result of the delivery of the services. In such circumstances, even if some Cayman residents are part of the list of data subjects that are processed, they are provided with GDPR data subject rights and no more. The processing of their personal data is due to the obligations under e.g. European anti money laundering legislation ("AMLD5") or depositary legislation ("AIFMD") on the non-Cayman Citco entity providing services to the Cayman fund or client entity. EEA established entities are subject to the GDPR by reason of Article 3(1) and so data subjects, irrespective of where in the world they are located, have GDPR rights. **Where Cayman DPL and GDPR contractual obligations both apply** If the Cayman fund ***does*** fall within the extra territorial scope of the GDPR and the fund finds itself within the scope of ***both*** the GDPR and Cayman law, it would result in GDPR Article 28 contractual assurance provisions being required to be entered into with service providers (in addition to its Cayman DPL contractual obligations).

III. Comparison between GDPR and Cayman DPL

Generally, the GDPR and DPL contain similar provisions. The table below outlines the differences.[1]

Subject	GDPR	Cayman DPL
Data Controller	The person who, alone or with others, determines the purposes, conditions and means of the processing of Personal Data	DPL applies to any Data Controller in respect of Personal Data (a) established and processed in the Cayman Islands; or (b) processed in the Cayman Islands otherwise than for the purposes of transit.[2]
Retention Period	Personal data should not be kept for longer than is necessary to fulfil the purpose for which it was originally collected. Controllers must inform data subjects of the period of time (or reasons why) data will be retained on collection.	Not a requirement under DPL. However, as with the GDPR, if there is no compelling reason for a Data Controller to retain Personal Data, a data subject can request its secure deletion. Personal data should not be kept for longer than is necessary to fulfil the purpose for which it was originally collected.
Data Security	Minimum security measures are prescribed as pseudonymisation and encryption, ability to restore the availability and access to data, regularly testing, assessing and evaluating security measures.	Appropriate technical and organizational measures must be taken to prevent unauthorized or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data.[3]
Data Processors	Security requirements are extended to data processors as well as Data Controllers.	There is no liability for processors under DPL. However, they may be held liable based on contract or tort law.
Data Breach	Data Controllers must notify the regulatory authority of Personal Data breaches without undue delay and, where feasible, not later than 72 hours after having become aware of a breach.	In the event of a Personal Data breach, the Data Controller must, "without undue delay" but no longer than five (5) days after the Data Controller should have been aware of that breach, notify the Ombudsman and any affected individuals.[4]
Direct Marketing and Consent	The Data Controller must inform individuals of their right to object "at the point of first communication" and in a data privacy notice (DPN). For any consent to be valid it needs to be obvious what the data is going to be used for at the point of data collection and the Data Controller needs to be able to show clearly how consent was gained and when it was obtained.	Including an unsubscribe facility in each marketing communication is recommended best practice. If an individual continues to accept the services of the Data Controller without objection, consent can be implied.

[1] Obtained from Loeb Smith
[2] See Art. 6 of the DPL
[3] See Schedule 1 of the DPL
[4] See Art. 16 of the DPL

Subject	GDPR	Cayman DPL
Data Processors	The GDPR sets out more detailed statutory requirements to apply to the controller/processor relationship, and to processors in general. Data Processors are now directly subject to regulation and are prohibited from processing Personal Data except on instructions from the Data Controller.	Best practice would always be to put in place a contract between a controller and processor. Essentially, the contract should require the Data Processor to level-up its policies and procedures for handling personal data to ensure compliance with DPL. Use of sub-contractors by the service provider should be prohibited without the prior approval of the Data Controller.[5]
Data Protection Officer	Mandatory if the core activities of the Data Controller consist of processing operations which require large scale, regular and systematic monitoring of individuals or large scale processing of sensitive Personal Data.	Does not require the appointment, although this is recommended best practice.
Penalties	Two tiers of sanctions, with maximum fines of up to €20 million or 4% of annual worldwide turnover, whichever is greater.	Refusal to comply or failure to comply with an order issued by the Ombudsman is an offence. Penalties are also included for unlawful obtaining or disclosing Personal Data.[6] Directors may be held liable under certain conditions.[7] The Data Controller is liable on conviction to a fine up to CI$100,000 or imprisonment for a term of 5 years or both. Monetary penalty orders of an amount up to CI$250,000 may also be issued against a Data Controller.

[5] Under DPL, the Data Controller is liable for breaches and non-compliance, whereas processors may not be. It is therefore very important for a funds BOD to ensure that adequate contractual protections are in place.
[6] See Arts. 53-54 of the DPL
[7] See Art. 58 of the DPL

IV. Data Protection Fact Sheet

Ten Steps To Take[8]	Citco's Response
1. Become aware	Face-to-face sessions were conducted in Citco Cayman to apprise staff of the new DPL coming into effect.
2. Know the data you hold	Data mapping was completed for all Citco applications
3. Privacy notices	Our DPN is available at www.citco.com/privacy and updated on a regular basis as required.
4. Individuals' rights	We have procedures in place to cover all the rights of individuals.
5. Subject access requests	This process has been documented and a procedure is already in place to deal with these requests
6. Legal basis of processing personal data	Generally, the conditions under which we process personal data are: contract, legal obligation or legitimate interest.
7. How to use consent	This is mostly required when processing personal data for marketing purposes. This is covered under existing procedures and with our existing application for marketing.
8. Data breaches	We have created a procedure specifically for Data Breaches. This will be used in the case of a breach affecting any Citco entity/Data Subject in any jurisdiction.
9. Data Privacy Impact Assessment (DPIA) and Privacy by Design and Default (PbDD)	DPIAs have been completed for all applications. PbDD framework created and in place; e-learning is mandatory for on-boarded IT staff and yearly thereafter. DPIA and PbDD has been incorporated in our Software Development Lifecycle.
10. Cross-border issues	Generally, the conditions under which we transfer personal data are for: The performance of a contract, legal obligation or legitimate interest. Citco has also executed an intra-group data transfer agreement which incorporates the model contractual clauses for the transfer of personal data to processors in third countries.

[8] Cayman Islands Ombudsman - https://ombudsman.ky/images/pdf/pol_guide/OMB-DP-Fact-Sheet-Ten-steps-20180529.pdf

The Citco Group Limited is the indirect parent of a network of independent companies. The Citco Group Limited provides no client services. Such services are provided solely by the independent companies within the Citco group of companies (hereinafter, the "Citco group of companies") in their respective geographic areas. The Citco Group Limited and the Citco group of companies are legally distinct and separate entities. They are not, and nothing contained herein shall be construed to place these entities in the relationship of agents, partners or joint ventures. Neither Citco Group Limited nor any individual company within the Citco group of companies has any authority (actual, apparent, implied or otherwise) to obligate or bind The Citco Group Limited in any manner whatsoever.

Citco DISCLAIMER

The information contained in this document is for informational purposes only. The information contained in this document is presented without any warranty or representation as to its accuracy or completeness and all implied representations or warranties of any kind are hereby disclaimed. Recipients of this document, whether clients or otherwise, should not act or refrain from acting on the basis of any information included in this document without seeking appropriate professional advice. The provision of the information contained in this document does not establish any express or implied duty or obligation between Citco and any recipient and neither Citco nor any its shareholders, members, directors, principals or personnel shall be responsible or liable for results arising from the use or reliance of the information contained in this document including, without limitation, any loss (whether direct, indirect, in contract, tort or otherwise) arising from any decision made or action taken by any party in reliance upon the information contained in this document.