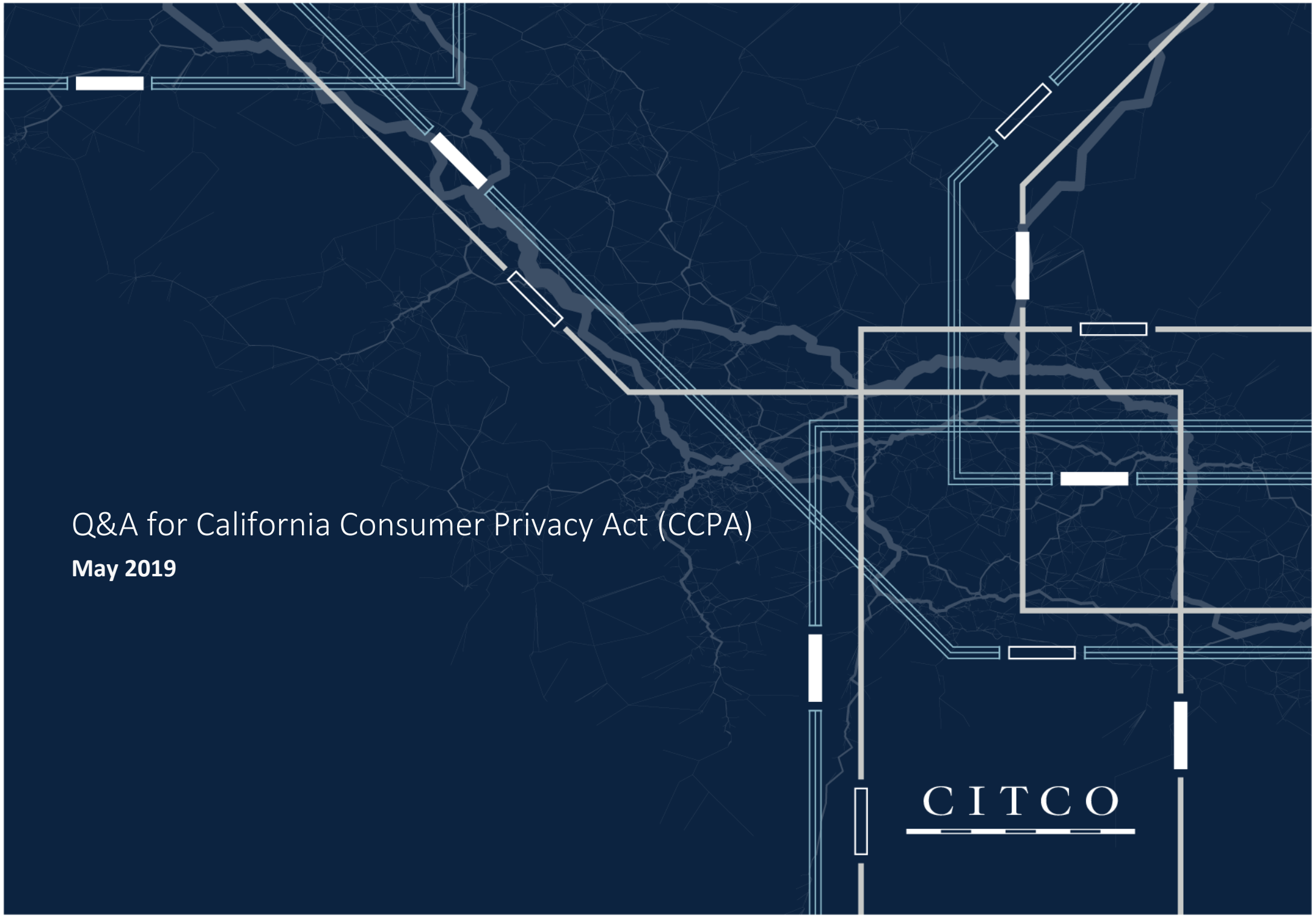

Q&A for California Consumer Privacy Act (CCPA)

May 2019

CCPA Requirements		Response / Comments
Definitions		
1.	What is considered “Personal Information”?	Personal information as defined in the CCPA is “Information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.” It includes information typically considered PII under state breach laws – names, unique personal identifiers, account names, social security numbers, driver’s license numbers, passport numbers, biometric information and “other similar identifiers.” It also includes aliases, IP addresses, “characteristics of protected classifications under California or federal law,” commercial information (defined to include personal property records or purchasing history), geolocation data, internet activity (including browsing and search history as well as web tracking data), professional and employment information, and education information. In addition, “personal information” includes “audio, electronic, visual, thermal, olfactory or similar information” and “inferences drawn” from any of the information contained in the definition. Examples include, but are not limited to, a person’s name, email address, IP address, biometric information, geolocation information, and profile information.
2.	What is the definition of a “consumer”?	A “consumer” is a natural person who is a California resident, whether or not the consumer is a customer of the covered business.

CCPA Requirements		Response / Comments
3.	What is the definition of a "California resident"?	In its definition of a "consumer", the CCPA relies on the definition of California resident which is used in tax legislation (Section 17014 of Title 18 of the California Code of Regulations). Therein, a "California resident" is defined as "*(1) every individual who is in the State for other than a temporary or transitory purpose, and (2) every individual who is domiciled in the State who is outside the State for a temporary or transitory purpose. All other individuals are non-residents*." The underlying logic of this definition is that the state in which an individual has the closest connection to during the taxable year is the state of that individual's residence. An individual may be resident but not domiciled in California, and conversely, may be domiciled in California without being a resident. The same tax legislation (Section 17014(b) and Section 17014(c) of Title 18 of the California Code of Regulations) clarifies what is meant by "a temporary or transitory purpose" and "domicile". To help establish whether an individual is indeed a California resident, Section 17014(b) provides that "*It can be stated generally…that if an individual is simply passing through this State on his way to another state or country, or is here for a brief rest or vacation or to complete transaction, or perform a particular contract, or fulfil a particular engagement, which will required his presence in this State for but a short period, he is in this State for temporary or transitory purposes and will not be a resident by virtue of his presence here.* *If, however, an individual is in this State to improve his health and his illness is of such a character as to require a relatively long or indefinite period to recuperate, or he is here for business purposes which will require a long or indefinite period to accomplish, or is employed in a position that may last permanently or indefinitely, or has retired from business and moved to California with no definite intention of leaving shortly thereafter, he is in the State for other than temporary or transitory purposes, and, accordingly, is a resident taxable upon his entire net income even though he may retain his domicile in some other state of country."*

CCPA Requirements		Response / Comments
4.	What is the territorial scope of the CCPA?	Like the GDPR, the CCPA affects businesses outside of the State of California to the extent they process data of California residents. Unlike the GDPR, the CCPA does not apply to businesses that "monitor the behaviour" of California residents (provided the activity cannot be considered to be doing business with California residents).
5.	Is there a concept of "Controller" and "Processor", similar to the GDPR?	The CCPA does not have the concept of "Controller" and "Processor" but instead refers to "Businesses" and "Service Providers" which have similar (but not identical) meanings. For example, in order to qualify as a "Business" under the CCPA, an entity must (among other things) "*determine…the purposes and means of the processing of consumers' personal information*" (language similar to that used in the GDPR to describe a data controller). In order to qualify as a "Service Provider" under the CCPA, an entity must (among other things) "*process information on behalf of a Business*". In addition to determining the purposes and means of the processing of consumers' personal information, to be regarded as a Business for the purposes of the CCPA, the entity must be a for-profit controller and meet one or more of three thresholds: - Annual gross revenue over $25 million USD; - Buys, sells, receives or shares for commercial purposes the data of 50,000 California residents; or - Derives 50% of revenue from "selling" personal data of California residents. Once an entity in a company group qualifies as a controller, parent companies and subsidiaries may automatically qualify as a Business even though they do not meet the thresholds or act as controllers. A Service Provider is a processor to a Business that receives the (California resident) data for business purposes under a written contract containing certain provisions and is a for-profit entity.

CCPA Requirements		Response / Comments
6.	Who is regulated by the CCPA?	Unlike the GDPR (which covers businesses, not-for-profit organisations and government entities), the obligations of the CCPA apply only to for-profit entities.
Data Location		
7.	Where is data stored?	The data is stored on Citco proprietary IT tools. Fund data is stored on servers based in the US; investor data is stored on the servers based in Switzerland. The data may be transferred to shared service centres and centres of excellence within the Citco Group as well as to approved sub-contractors.
Overall Approach to Compliance		
8.	How do the GDPR and CCPA compare?	GDPR requirements are stricter than the upcoming CCPA as well as most other privacy regulations throughout the world. The GDPR sets out approximately 55 technical and organizational measures with which organizations must comply. (The CCPA sets out just 9 technical and organization measures with which organizations must comply.)
9.	Does Citco fall in scope of the CCPA?	Ordinarily, Citco (including its group of companies) would not recognise itself as being a "Business" for the purposes of the CCPA and so would not come within the scope of the CCPA in its own right. Where a client is a "Business" and relies on Citco to provide services to the client which involves the use of Personal Information, Citco may, in that context, be recognised as a Service Provider. However, not all vendors of services are considered Service Providers under the CCPA. In addition to an entity processing personal information "on behalf of a Business", the entity must be subject to a contract that prohibits it from retaining, using or disclosing the personal information "*for any purpose other than for the specific purpose of performing the services specified in the contract*". Where the terms of the services agreement in place between the client and Citco necessarily provides for retention of Personal Information beyond termination, allows the use of personal information (in any form) for its own

		purpose, or allows the vendor to make decisions about disclosure of personal information, the definition of "Service Provider" under the CCPA would not be met. Citco (and other similar service providers) work under a range of professional obligations that oblige it to take responsibility for the personal information it processes (e.g. anti-money laundering legislation). In order to meet the requirements of such obligations, Citco, from time to time, would not be acting on the client's instructions (as set out in the relevant service agreement) but instead in accordance with its own professional obligations and therefore for its own purpose.
10.	Do you have a programme for achieving compliance with the CCPA?	Yes. Citco established a Data Privacy programme in 2016 to oversee the implementation of GDPR. This programme contained representatives from all business divisions and from group functions such as legal, risk, compliance and IT. From May 25th 2018 the programme transitioned fully into the Citco Data Privacy function lead by the Chief Privacy Officer. Citco has taken the approach to apply the GDPR requirements across all of its applications and business processes throughout the organization (the GDPR is our "golden standard" for how we handle data privacy). To the extent that Citco is within the remit of the CCPA, most of the compliance measures that are required under the CCPA have been examined and actioned while achieving compliance with the GDPR.
11.	Please state the name and position within the company of the individual with overall responsibility for implementation of the CCPA.	Mike Piccirilli – Chief Privacy Officer ("CPO").
12.	What is the legal basis for a business to collect and sell personal information?	The CCPA does not list the legal grounds on which Businesses can collect and sell personal information. It only provides that Businesses must obtain the consent of consumers when they enter into a scheme that gives it financial incentives to sell that information.

CCPA Requirements		Response / Comments
Principles relating to processing of personal data		

13.	What are my rights as a California consumer?	• Right to know regarding
		  ○ categories of personal information collected;
		  ○ specific pieces of personal information collected;
		  ○ the business purpose for the collection;
		  ○ the categories of sources for the information; and
		  ○ the categories of 3rd parties that purchased or otherwise receive consumer's personal information
		• Right to say no (opt out of having information sold to a third party)
		• Right to have personal information deleted except under certain conditions as outlined in the CCPA
		
		The consumer can exercise these rights via requests to the Business. If necessary, the Business in turn will contact the Service Provider to take the appropriate action.

14.	Are there measures in place in order to ensure that data collected is used for the explicit purposes that the data was collected for?	Citco adheres to this principle and ensures that its staff is aware that data is used for the explicit purpose for which it was collected. Before using data for a different purpose, Citco would inform the relevant consumers and/or clients in advance.
Security of Processing		
15.	Please confirm how you will implement appropriate technical and organisational measures for ensuring that, by default, only personal data which is necessary for each specific purpose of processing is collected, stored and processed?	Confirmed. In accordance with the principle of data minimisation, Citco will only request such personal data from our client which is required for one of the specified purposes. While personal data is in our possession, should there be any changes affecting the manner in which such data is collected, stored or processed, such changes will be subject to a Data Privacy Impact Assessment and sign off by Citco's Chief Privacy Officer prior to any change being implemented.

CCPA Requirements		Response / Comments
16.	**What are Citco's technical and organisational measures to ensure a level of security appropriate to the risk?**	
	(a) the encryption of personal data;	Citco has implemented encryption of data in transit. The extent and nature of encryption which Citco implements is kept under review taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing.
	(b) the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services;	Please refer to controls below. Citco has also obtained an ISO 27001:2013 certification of our Information Security Management System ("ISMS" aka Security Program) in December 2016. The 27001:2013 is an industry standard framework for securing an ISMS. It is comprised of a suite of activities (14 domains) relating to the identification and management of information risks. An ISMS is a systematic approach to managing personal information so that it remains secure. It includes people, processes and IT systems by applying a risk management process. The certification applies Citco group-wide and covers all Citco computer systems/IT operations - used by all entities within Citco. Citco's offices with significant IT presence/operations are in scope of the certification as certain aspects of the certification are specific to where these operations take place. We can supply you with a copy of our certificate upon request.
	(c) Ensuring processes exist to manage access controls to 'least privilege'	Changes to access must go through our Change Management system which requires management sign off. User attestations are reviewed by managers every quarter.
	(d) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;	Our systems are clustered (high availability). We also maintain a separate facility in the event the facility goes off-line. Complete failover is tested annually.

CCPA Requirements		Response / Comments
	(e) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.	Citco has implemented and maintains physical, electronic and procedural safeguards and security measures, which are designed to protect your personal information. For example: • Encryption; • Citco operates under the principles of Least-privilege and Segregation of Duties; • Multi-factor authentication to access external-facing web servers; • Advanced Persistent Threat Infrastructure; • Firewalls In all offices and Data Centres; • Privileged Access Control; • Threat Intelligence Services; • Intrusion Detection Systems (IDS) in all offices and Data Centres; • System Protection including Anti-virus/Anti-spam, Heuristic Detection, HIPS, etc.; • Email Infrastructure - Highly available (clustered); • Data Loss Prevention systems; • Security part of Lifecycle development process; • Code reviews and penetration tests conducted during development and prior to production release; • Baseline security established for systems and periodically measured for compliance; • Developers do not have access to production systems; • 3rd party Data Centres professionally managed and maintained; Badge reader or biometric authentication required to access offices or computer rooms.
17.	Are you already certified or do you plan to a use certification scheme (pursuant to Article 42) such as ISO 27001 to serve the purpose of demonstrating that the organisation is actively managing its data security?	We obtained ISO 27001:2013 certification of our Information Security Management Systems (“ISMS”) in December 2016.

CCPA Requirements		Response / Comments
Notification of a Personal Data Breach to Business and/or Consumer		
18.	Does Citco have a process in place to ensure that the Business and/or consumer is notified in the most expedient time possible and without unreasonable delay after Citco has become aware of a personal data breach?	Yes. We have a process in place that includes the Citco Privacy Evaluation Team to immediately analyse the breach and issue recommendations with regard to the appropriate actions to take.