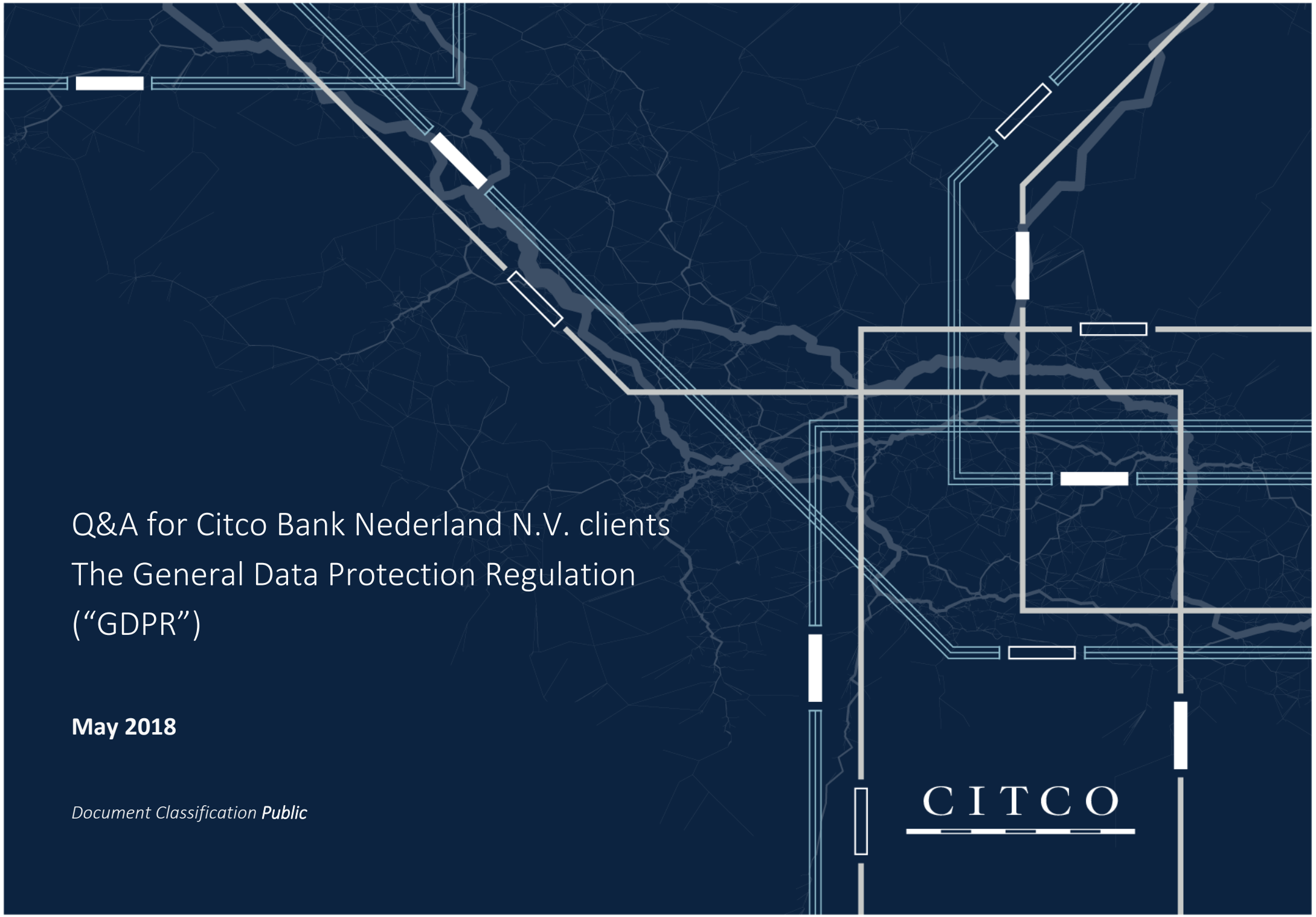

Q&A for Citco Bank Nederland N.V. clients The General Data Protection Regulation ("GDPR")

May 2018

Document Classification ***Public***

CITCO

Q&A for clients of Citco Bank Nederland N.V. ("CITCO") in relation to the General Data Protection Regulation ("GDPR")

	GDPR Requirements	Response / Comments
Overall Approach to Compliance		
1.	Do you have a programme for achieving compliance with the GDPR?	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 will transition fully into the Citco Data Privacy function lead by the Chief Privacy Officer.
2.	Please state the name and position within the company of the individual with overall responsibility for implementation of the GDPR	Mike Piccirilli – Chief Privacy Officer ("CPO")
3.	Have you: • Completed a gap analysis and determined the work required for compliance? • Secured the necessary budget and resource needed? • Established a project plan that will ensure compliance by the required deadline?	• A gap analysis has been conducted between the current approach and the requirements under GDPR. • The Citco Group has allotted all the necessary resources (staff and budget) to its GDPR project. • The project plan is on track and to ensure compliance when the GDPR enters into force.
Definitions and Data Location		
4.	With regard to the contract you have, do you believe yourself to be the Data Controller, Joint Data Controller or Data Processor?	When providing banking and/or depositary services, Citco considers that it is a Data Controller by virtue of the fact that we will determine the purposes and means of the processing of personal data in order to comply with our legal and regulatory obligations, such as anti-money laundering and know your customer obligations, filing of suspicious transaction reports (STR), obligations following AIFMD, PSD2 and any other applicable legal, tax or regulatory obligations.

GDPR Requirements		Response / Comments
5.	Please state where your data is stored. Please advise if it is held: • within the UK; • within another country in the EU / EEA; • a country that has Adequacy status or; • Stored in a Third Country? In answering this question please consider the location of your systems, servers / datacentres and also those of your sub-contractors / suppliers where they have access to our personal data, including any software and cloud service providers.	The data is stored on Citco proprietary IT tools, the servers for which are based in Switzerland. Switzerland is a country that has Adequacy status. The data is transferred to shared service centres and centres of excellence within the Citco Group as well as to approved sub-contractors. All relevant Citco Group entities have executed an intra-group data transfer agreement, which incorporates the model contractual clauses for the transfer of personal data to processors in third countries as set out under European Commission 2010/87/EU of 5 February 2010, to ensure that your personal information is treated by our Citco affiliates outside the EU in a way that is consistent with and which respects the EU laws on data protection. The transfer of personal data to sub-contractors outside the EU/EEA is also either to a country that has Adequacy status, or subject to data transfer agreements which incorporate the model contractual clauses for the transfer of personal data as above.
Article 5 & 14– Principles relating to processing of personal data		
6.	Are there measures in place in order to ensure that data collected will only be used for the explicit purposes that the data was collected for?	Citco adheres to this principle and ensures that its staff is aware that personal data may only be used for the explicit purpose for which it was collected. Before using personal data for a different purpose, Citco would inform the relevant data subjects in advance in accordance with article 14 GDPR.

GDPR Requirements		Response / Comments
Article 25 – Data Protection by Design and by Default		
7.	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? In answering this question, please outline how GDPR considerations are embedded within your project and change processes; including requirements to complete Privacy Impact Assessments (PIA) in all appropriate cases.	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 CPO prior to any change being implemented.
8.	Please also confirm what steps you have implemented to meet the requirements of Article 25 (implementing data protection by design and by default) in order to protect the rights of data subjects?	We have incorporated Privacy by Design and Default into our software development lifecycle and all application development staff have reviewed and received guidance on this framework

GDPR Requirements		Response / Comments
Article 28 – Processor		
9.	Where Citco (as controller) uses a third party to carry out certain processing on its behalf (a processor), please confirm that Citco shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject.	Confirmed. Please note that where Citco intends to outsource any tasks to a Citco affiliate, such Citco affiliate shall adhere to equivalent technical and organisations measures in a manner consistent with the requirements of the GDPR To the extent that Citco intends to engage any third party service providers, Citco shall conduct a due diligence assessment prior to engaging such third party to ensure that they are able to provide sufficient guarantees.

GDPR Requirements		Response / Comments
10.	Contractually Citco must ensure that all persons authorised to process personal data are under an appropriate obligation of confidentiality and this is enforced through contractual agreements. What are you doing to ensure that the contract governing the processing of data between Citco and any processors engaged by Citco will include the requirements and stipulations stated in Article 28(3) of the GDPR?	Our GDPR contract has been drafted by external counsel competent to advise on GDPR and, amongst other things, includes provisions which requires the processor to: • only act in accordance with the controller's documented instructions; • impose confidentiality obligations on all personnel that process the relevant data; • ensure security of the data that the processor processes; • comply with the rules regarding appointment of any sub-processors; • implement measures to assist the controller in complying with the rights of the data subjects; • at the controller's discretion, return or destroy personal data at the end of the relationship except as required by applicable law; and • provide the controller with all information necessary to demonstrate compliance with the GDPR.
Article 30 – Records of Processing Activities		
11.	Please confirm that you will maintain an updated record of all categories of processing activities carried out by you including the requirements stipulated in points (a) - (d) under Article 30 Para 2. Do you have a plan for identifying where personal data is stored within your organisation and to keep records of the storage location and of any data transfers (Please provide an outline of the solutions to be implemented).	Confirmed. We have performed data mapping on applications where personal data is transferred/stored as well as the categories of processing activities as required under Article 30 Para 2.
Article 32 – Security of Processing		
12.	Please confirm if you are aligned with Article 32 of the General Data Protection Regulation, and that you shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including the requirements stipulated in points	

GDPR Requirements		Response / Comments
	(a) - (d) under Article 32 Para 1. Please advise your current arrangements or future enhancement plans in the following areas;	
	(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 sensitive 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.

GDPR Requirements		Response / Comments
	(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.
	(e) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.	We regularly test a number of controls for effectiveness and security of processing. Tests are conducted by 1st line of defence (business). Results are overseen by Risk Management – 2nd line of defence. Risk framework is audited by internal Group audit – 3rd line of defence. In addition, we have dedicated security staff who test all systems for vulnerabilities. All systems are tested after each patch cycle; after any significant changes; prior to new systems going into production. Citco also has an independent 3rd party conducting tests on an annual basis of our DMZ environment. 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.;

GDPR Requirements		Response / Comments
		• 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.
13.	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.
Article 33 & 34 – Notification of a Personal Data Breach		
14.	Please confirm that you have a process in place to ensure that: (a)the competent supervisory authority is notified without undue delay after Citco has become aware of a personal data breach (unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons); and (b) where a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, you will communicate the personal data breach to the data subject without undue delay.	Confirmed

GDPR Requirements		Response / Comments
Article 35 – Data Protection Impact Assessment		
15.	Please confirm that you will conduct a Data Protection Impact Assessment as prescribed by Article 35 para 1 of the GDPR	Confirmed.
16.	Please confirm you will also assist in carrying out periodic reviews to ensure processing continues to be performed in accordance with the Data Protection Impact Assessment?	Confirmed.
Article 37 – Designation of the Data Protection Officer		
17.	Please confirm you will be aligned with Article 37 of the General Data protection Regulation. Do you have a designated Data Protection Officer, appointed on the basis of professional qualities and with expert knowledge of data protection law and practices, with the ability to fulfil the tasks referred to in Article 39.	Confirmed. Citco has designated a Chief Privacy Officer who oversees our data protection compliance. Our Chief Privacy Officer has the following certifications: CIPM, CISSP, CISA, CISM, CRISC, CGEIT, CSX-F

GDPR Requirements		Response / Comments
Article 44 – General Principles for Transfer		
18.	Please confirm that you have understood and will comply with Chapter 5 - Transfers of personal data to third countries or international organisations (includes Articles 44 - 50), including the general data transfer principles covering: • Transfer of personal data which are undergoing processing or are intended for processing after transfer to a 'Third Country' or to an international organisation • Onward transfers of personal data from the Third Country or an international organisation to another third country or to another international organisation. NB: 'transfer' includes data being processed in a third Country or by an international organisation (data does not need to be **physically** stored there).	Confirmed. The Citco affiliates have executed an intra-group data transfer agreement which incorporates the model contractual clauses for the transfer of personal data to processors in third countries as set out under European Commission 2010/87/EU of 5 February 2010, to ensure that your personal information is treated by our Citco affiliates outside the EU in a way that is consistent with and which respects the EU laws on data protection. Where the transfer of personal data is made to a Third Country outside the EU/EEA and is not a country that has Adequacy status, data transfer agreements are in place which incorporate the model contractual clauses for the transfer of personal data as above.
19.	The Commission has so far issued two sets of standard contractual clauses for transfers from data controllers to data controllers established outside the EU/EEA and one set for the transfer to processors established outside the EU/EEA. Please confirm if you will be willing to adopt /comply with the relevant EU model clauses for data transfer if required to do so where data is held outside the EU/ EEA (and also apply this to your sub-contractors).	Confirmed.

GDPR Requirements		Response / Comments
20.	What post Brexit contingency plans are your organisation making to minimise GDPR compliance risks? Which solutions has your firm considered to maintain these activities (e.g. model contract clauses, binding corporate rules, new data centres)?	The UK has now updated its data protection legislation to take into consideration GDPR. We believe that post Brexit, the EU Commission will designate the UK as an equivalent jurisdiction and therefore data transfers to the UK will be permitted and protected. Should the Commission not grant a decision of adequacy to the UK, we will work with our clients on a suitable solution to permit personal data to be transferred to the UK.
21.	Please confirm if you are planning to update your policies for GDPR compliance?	A set of GDPR-compliant policies has already been adopted. These policies are subject to periodic review.