GIBRALTAR FINANCIAL SERVICES COMMISSION

DLT Provider Guidance Notes

Financial Crime

Introduction

The purpose of this guidance note is to provide a DLT Provider, as defined in the Financial Services (Distributed Ledger Technology Providers) Regulations 2017 (the DLT Regulations), with guidance as to the operational, technical and organisational standards expected and in some circumstances required by the GFSC.

This guidance note is specifically in respect of the regulatory principle under paragraph 8 of Schedule 2 of the DLT Regulations (the Regulatory Principle).

The Regulatory Principle states that "***A DLT Provider must have systems in place to prevent, detect and disclose financial crime risks such as money laundering and terrorist financing".***

This document should be read as interpretative guidance for a DLT Provider and the examples contained in this document should be noted as indicative of good practice by a DLT Provider in connection with the Regulatory Principle.

A DLT Provider should note that the GFSC will take this document into account when reviewing a DLT Provider's practices. The operational standards expected and required by the GFSC of a DLT Provider will vary depending on the size, particular nature, scale or complexity of the DLT Provider's business.

Scope and Applicability

A DLT Provider is defined as providing a Controlled Activity under the Financial Services (Investment and Fiduciary Services) Act and is therefore caught as a relevant financial business under the Proceeds of Crime Act (POCA).

The GFSC's Guidance Notes on 'Systems of control to prevent the financial system from being used for Money Laundering or Terrorist Financing activities' (AMLGNs) also apply to a DLT Provider.

These additional notes provide sector specific guidance on mitigating measures and provides the risk context for this sector.

Risk and Context

Recent analysis of the threats and risks posed by virtual currencies in the European Union point to vulnerabilities due to the anonymity in the exchange between fiat currencies and virtual currencies and the holding of virtual currencies in an unregulated environment. By subjecting a DLT Provider to regulation and supervision and applying POCA to their activities, Gibraltar seeks to mitigate these risks considerably.

Specific Measures

In addition to the provisions of the AMLGNs, the following additional measures should be applied when a DLT Provider is establishing a business relationship or executing a one-off transaction. These additional mitigation measures are designed to be technology neutral.

B2B versus B2C

A DLT Provider may be providing services and products to both Business to Business (B2B) and/or Business to Consumer (B2C) segments. Whilst the know your customer (KYC) requirements of POCA apply, it is important to differentiate on a risk-based approach, between the risks presented by both of these in the context of money laundering and terrorist financing risks. A DLT Provider must document its risk tolerance and assessment carefully for each of the products or services it offers in accordance with Chapter 6 of the AMLGNs.

Irrespective of the type of product or service provided, if there is a knowledge or suspicion of money laundering or terrorist financing, the obligation to submit a Suspicious Activity Report (SAR) under POCA applies.

B2B

In respect of B2B, it is very important for a DLT Provider to know the nature of its client's business, the managers and business owners and the manner in which they operate.

A DLT Provider providing services or products on a B2B basis, which does not offer conversion of fiat currencies to any type of stored value and vice-versa, need not apply the transaction monitoring requirements of the AMLGNs to the B2B's underlying customers. However, the legal requirements contained in POCA shall continue to apply.

DLT Providers are not expected to have access to data relating to the customers of their B2B clients or request the same for money laundering or terrorist financing purposes. However, monitoring of B2B clients should include monitoring to ensure "*that the transactions are consistent with the relevant financial business's or person's knowledge of the customer, his business and risk profile, including where necessary the source of funds and keeping the documents, data or information obtained for the purpose of applying customer due diligence measures up-to-date*", as set out in Section 12(2) of POCA.

B2C

Where the product or service has an element of storage and/or remittance of value, which can be converted to, or from fiat currencies, be this in cash or via more traditional transfer mechanisms, the AMLGNs will apply.

Customer Due Diligence and Know Your Customer

The customer due diligence measures (CDD) and KYC requirements of POCA apply to a DLT Provider. However, the GFSC is keen to support new technologies and the emerging use of information and data to carry out due diligence (and not just reliance on documents) that enable easier management of CDD (see further below).

The GFSC will take a view on the adequacy of any new technologies used to support a DLT Provider to comply with its CDD and/or KYC obligations as part of the application process and in the context of a DLT Provider's business, product(s) and/or service(s).

A DLT Provider will be required to comply with CDD as set out in Part III of POCA. The GFSC will only expect firms to apply simplified due diligence for transactions under €150, or equivalent. The GFSC will consider representations made on a case by case basis, to allow simplified due diligence for transactions greater than €150, only if a DLT Provider has:

- made a comprehensive risk assessment that determines that the transaction, product or service is deemed to be low risk; and
- it considers that it has sufficiently robust systems of controls.

Nonetheless, the traceability principles below need to be complied with in order to determine if one or more transactions are linked and this limit would be breached. Similarly, if money laundering or terrorist financing is known or suspected, full KYC and SAR requirements apply.

eID for Verification of CDD Measures

The objective of CDD is to properly identify and verify parties (whether natural or legal persons) to a transaction or payment. Therefore, electronic identification and trust services (governed by the eIDAS Regulation - EU Regulation no 910/2014) are relevant when opening a business relationship with a DLT Provider. Currently the eIDAS framework is one of the cornerstones of the Digital Single Market covering all elements of an electronic identification and authentication. A list of designated bodies, certified qualified signature creation devices, and certified qualified seal creation devices can be found here.

Where POCA refers to identifying and verifying a customer's identity on the basis of documents, data or information obtained from a reliable source, this should be read as also including electronic identification and relevant trust services as set out in Regulation 910/2014.

Traceability

A DLT Provider must know the identity of each and every customer and not process transactions where it does not know the customer's identity.

A DLT Provider must keep records of customer details and transactions including those on a distributed ledger so that holdings and transactions can be traced to each customer. These records must form part of the document retention processes of the DLT Provider and must be retained for a minimum of five years after the end of the business relationship or one-off transaction.

A DLT Provider should capture, record and retain unique identifiers of devices and network connections used by customers in communicating with the DLT Provider. Unique identifiers include (without limitation) IP address, MAC address, IMEI, ICCID, MEID, SEID and UUID. Recorded unique identifiers should form part of the document retention processes of the DLT Provider.

A DLT Provider should have systems to detect attempts by customers to circumvent CDD requirements or to obfuscate the nature and purpose of transactions. As part of its transaction monitoring processes, a DLT Provider should have systems to detect incongruity between information known about or provided by customers and information gathered during transactions. Incongruities and anomalies should be flagged, investigated and risk assessed for financial crime purposes.

GIBRALTAR FINANCIAL SERVICES COMMISSION

Published by:
Gibraltar Financial Services Commission
PO Box 940
Suite 3, Ground Floor
Atlantic Suites
Europort Avenue
Gibraltar

www.gfsc.gi