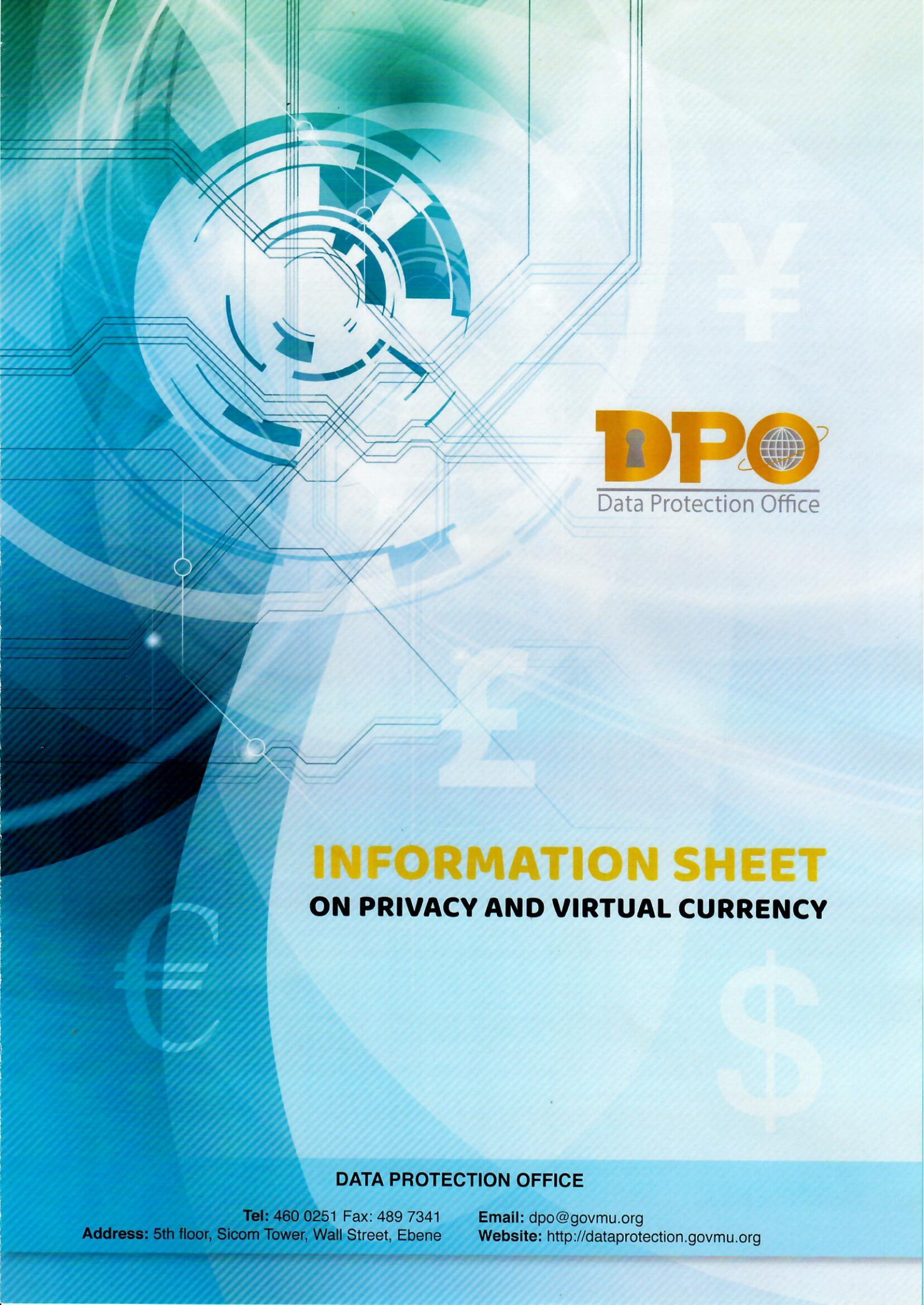

DPO
Data Protection Office

INFORMATION SHEET
ON PRIVACY AND VIRTUAL CURRENCY

DATA PROTECTION OFFICE

Tel: 460 0251 Fax: 489 7341
Address: 5th floor, Sicom Tower, Wall Street, Ebene

Email: dpo@govmu.org
Website: http://dataprotection.govmu.org

1. WHAT IS A VIRTUAL CURRENCY?

A virtual currency is a digital representation of value, which can be transferred, stored or traded electronically. It is not issued by a central bank nor a public authority but is usually issued, managed and controlled by its developers. It is accepted as a means of exchange among the members of a virtual community.

Example: BITCOIN

Bitcoin uses a cryptographic and a distributed data structure technology called blockchain.

2. DOES THE DATA PROTECTION ACT (DPA) APPLY TO THE PROCESSING OF VIRTUAL CURRENCIES?

As a rule of thumb, the DPA applies to the processing of personal data. Personal data refers to any information relating to an identified or identifiable individual, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.

The DPA will thus apply in circumstances where individuals can be identified directly or indirectly when undertaking transactions using virtual currencies.

3. WHAT ARE THE PRIVACY RISKS OF VIRTUAL CURRENCIES?

Virtual currency transactions occur solely on the Internet and are prone to cyber security threats such as online theft. Generally, virtual currencies are stored in computer accounts called virtual wallets. These wallets are often the target of hackers which consequently reduce trust in virtual currency systems.

The identity of users on virtual currency platforms are usually pseudonymous in nature. This implies that users do not know each other's identity when transacting. Nevertheless, any user can still view the full history of transactions of pseudonymous users on a virtual ledger which is publicly available for anybody to view. This makes virtual currency systems particularly sensitive to anonymity breaches that could potentially reveal the full history of transactions of a user if his identity is unmasked. For instance, an anonymity breach to identify users could happen by obtaining the mailing addresses for the delivery of purchased goods.

Whilst data protection laws require the processing of personal data to be transparent to users using plain and simple language, the realm of virtual currency systems is complex and not fully comprehended by individuals.

4. PRIVACY AND DATA PROTECTION ISSUES IN VIRTUAL CURRENCY SYSTEMS

Many virtual currency systems use blockchain technology where the following issues may be encountered:

Role Identification Issues **Who is the controller/processor? (challenging issue in a distributed ledger scenario)**	The decentralised data governance model used in blockchain technology together with the multitude of actors involved in the processing of data lead to a more complex definition and identification of their roles, obligations and accountability within such data structure models.
Obligations of controllers/ processors and Rights of data subjects (rectification, erasure, restriction)	Data protection laws impose certain obligations on controllers/ processors to: • process personal data fairly and in a transparent manner, • ensure security of data, • permit the correction of inaccurate personal data, • ensure destruction of data when the purpose for keeping personal data has lapsed. These obligations are difficult to comply with in a blockchain environment where a new block is added permanently and cannot be altered.
Jurisdictional issues	In a cross-border decentralised blockchain environment, it is difficult to identify which jurisdiction's law and regulation would apply.

5. PRINCIPLES OF DATA PROCESSING

The foundational principles related to the processing of personal data must be observed in any technological system including the virtual currency system. Under the Mauritius Data Protection Act 2017, controllers and processors must ensure that personal data are:

(a) **processed lawfully, fairly and in a transparent manner in relation to any data subject**

(b) **collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes**

(c) **adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed**

(d) **accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data are erased or rectified without delay**

(e) **kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed**

(f) **processed in accordance with the rights of data subjects**

6. RECOMMENDATIONS

The primary responsibility of virtual currency systems remains with entities that fund, develop and deploy such systems. Ethical standards should at the foundation of measures be adopted and inbuilt in the design of such platforms. The following recommendations have been formulated to minimise risks and improve the design and use of virtual currency systems.

a Transparency and fairness

- The service must be transparent to individuals using plain and simple language. This implies that all relevant information must be provided to individuals on how their data will be processed and any potential privacy risks during the processing. Moreover, assurance must be given that only minimum data will be collected with respect to the purpose/s for the execution of the service.

b Identification of controller

- The organisation(s) responsible for virtual currency systems must be made known to users with its/ their contact details.

c Accuracy and reliability

- Organisation(s) responsible for virtual currency systems must ensure that the processing of personal data is fair, accurate and reliable.
- If a virtual currency system uses blockchain data structures, then its developers must address the irreversibility nature of exchanges in such systems since data once uploaded cannot be deleted, altered or disputed. Mechanisms should be explored to correct inaccurate transactions or to handle disputes. Furthermore, permissioned blockchains should be favoured as they provide different types of permissions to participants such as Read (who can access the ledger and see transactions), Write (who can generate transactions and send them to the network), and Commit (who can update the state of the ledger).

d Security

- Organisation(s) responsible for these systems must safeguard data and processing operations against cybersecurity threats.
- The use of anonymisation techniques is encouraged to prevent the risks of identifying users.
- All transfers of data across jurisdictions must be secured with appropriate security measures.

e Privacy by design

- Organisation(s) must incorporate built-in privacy protections using data protection by design and default techniques to ensure that these systems do not pose risks to the rights and freedoms of individuals. Systems must be developped and also work in tandem with people's privacy expectations and rights.

f Data Protection Impact Assessment (DPIA)

- Organisation(s) responsible for virtual currency systems should carry out a DPIA to assess, evaluate and mitigate privacy risks.

g Rights of individuals

- The implementation of virtual currency systems must be in line with privacy rights of individuals. For instance, data protection laws recognise a right to erasure which enables an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

7. REFERENCES

1. *The Digital Agenda of Virtual Currencies, 'Can BitCoin Become a Global Currency?' By d'Artis Kancs, Pavel Ciaian and Miroslava Rajcaniova, 2015, Joint Research Center*
2. *Virtual currencies in the Eurosystem: challenges ahead, Monetary Dialogue July 2018, by the Policy Department for Economic, Scientific and Quality of Life Policies, Directorate-General for Internal Policies, PE 619.020 – July 2018*
3. *Commission Nationale Informatique & Libertes (2018) 'Solutions for a responsible use of the blockchain in the context of personal data'*