GRA

GIBRALTAR REGULATORY AUTHORITY

BLOCKCHAIN

Discussion paper regarding blockchain and the EU General Data Protection Regulation 2016/679 and the Data Protection Act 2004

20th February 2020

IR05/19

FOREWORD

The EU General Data Protection Regulation 2016/679 (the "GDPR") came into force on 25th May 2018, replacing the existing data protection framework under the EU Data Protection Directive 95/46/EC.

Her Majesty's Government of Gibraltar amended the Data Protection Act 2004 (the "DPA") on 25th May 2018, in accordance with the introduction of the GDPR. The DPA complements the GDPR and also implements the Law Enforcement Directive 2016/680. Therefore, the DPA and the GDPR must be read side by side.

It is important to note that the GDPR does not generally require transposition (EU regulations have 'direct effect') and automatically became law in Gibraltar. Therefore, organisations involved in the processing of personal data need to be aware of the obligations that the GDPR and/or the DPA will impose on them. The GDPR emphasises transparency, security and accountability by data controllers, while at the same time standardising and strengthening the right of European citizens to data privacy.

The Gibraltar Regulatory Authority, as the Information Commissioner, is aware of the increased obligations that the GDPR and DPA place on organisations. The Information Commissioner's aim is to alleviate some of the concerns for businesses, public-sector and third-sector organisations and assist them ensure data protection compliance.

CONTENTS

SUMMARY

- Blockchain is a decentralised system, which allows for the collection, storage and processing of data using distributed ledger technology (also known as DLT). This type of technology is able to facilitate transactions whilst eliminating the need for a centralised operator.

- Notwithstanding potential to encourage economic growth and benefit transactional processes, blockchain also brings about a new paradigm of data storage and governance that may create risks to data protection.

- The GDPR places an obligation on those processing personal data, rather than on infrastructure such as blockchain technology itself.

- Any natural person who enters personal data onto a blockchain for reasons unrelated to commercial or professional activity, e.g. buying or selling cryptocurrency for personal reasons, may be exempted from compliance with the GDPR by the 'personal and household exemption'.

- Both transactional data, as well as public keys, could fall within the GDPR's definition of personal data.

- Potential tensions between the GDPR and blockchain:

    - Identifying the data controller (and often also processor). The GDPR requires the identification of a data controller who will be accountable for compliance with the GDPR. However, as blockchain relies on a decentralised model, individuals and entities transact directly with each other, and there are often many contributing parties, blurring the certainty of an identifiable controller.

    - The anonymisation of personal data. The debate as to what it takes to fully anonymise personal data to such a standard whereby it can be stored on the blockchain whilst remaining anonymous remains open. For example, it has not yet been concluded that hashing can be considered a sufficient form of anonymisation of data in all circumstances.

    - Data subject rights and legal bases.

        - Article 5 of the GDPR. Potential tensions exist in relation to the principles of data minimisation, purpose limitation and storage limitation.

        - Article 6 of the GDPR. Difficulties in regard to reliance on consent (e.g. the inability to withdraw consent) and contract (e.g. inability to identify a data controller may impede a contract being established) as legal bases.

        - Article 15 of the GDPR. If it is not possible to identify the data controller, the individual has no point of contact and may be unable to exercise this right.

        - Articles 16 and 17 of the GDPR. Blockchain immutability impedes the right to rectification or to erasure.

- Article 19 of the GDPR. Notification of any rectification or erasure of personal data to other recipients is challenging considering the potential for a widespread blockchain.

- Article 22 of the GDPR. Use of smart contracts conflicts with the GDPR in its aims to protect individuals against legal or other significant effects arising from profiling or decision-making solely by a machine. Human intervention should be made possible to allow data subjects to contest the decision, even if the contract has already been performed.

- Data protection options and opportunities with blockchain:

  - Transparency. Provided a controller is identified, the obligations on said controller are arguably reasonably able to be actioned and should therefore not be an issue.

  - Technological developments. The ongoing evolution of blockchain can be seen as an opportunity for the technological development to be influenced early on for it to accommodate legal requirements, such as those associated with data protection.

  - Data governance and data sharing. Data subjects are arguably provided with a higher level of control over their personal data, and a medium by which to themselves share data with the intended recipient when required and only when they deem appropriate to do so.

  - Data storage off-chain. There are instances in which each entity could manage the personal data of its customers 'off-chain' and use blockchain to transact other business in a faster, cheaper way, without having to publish individual transactions.

  - Security. There are some inherent features within blockchain that could be considered positive security aspects of the technology. For example, having multiple copies of data may be considered as eliminating the risks associated with potential loss from one single point of failure, as well as making unwarranted tampering a more onerous feat.

- In the absence of conclusive court decisions, regulatory guidance is useful to provide greater legal certainty.

1. INTRODUCTION

Blockchain technology has rapidly become the most well-known application of distributed ledger technology globally. Its uses have become increasingly far reaching, with its extension into all major sectors across Europe. Its presence is found in 19% of Government services and 14.9% of financial services. 2.53% of health and pharmaceutical sectors are also making use of this technology in order to trace the origins of goods in a reliable manner[1].

Taking into consideration the irrefutably growing impact of blockchain technology on our social, economic and political domains, and given that blockchain and the EU General Data Protection Regulation 2016/679 ("GDPR") are sometimes perceived to be incapable of co-existence[2], it is imperative that their interaction, and the implications of blockchain technology usage when processing personal data, are considered.

This paper outlines key issues regarding the relationship between blockchain and the GDPR as understood by the Information Commissioner (the "Commissioner")[3]. Beyond outlining the Commissioner's initial views, the main purpose of the paper is to facilitate discussion and engagement with various stakeholders in his efforts to collaborate, examine and address data protection issues within the area of blockchain.

The paper reflects on the European Union's ("EU") general acceptance of the new technology but highlights potential tensions between blockchain usage and the GDPR as well as data protection options and opportunities when using blockchain.

[1] 'Next Generation Internet Brochure', European Commission, 18 September 2019 - https://ec.europa.eu/digital-single-market/en/news/next-generation-internet-brochure - last accessed 18 February 2020.

[2] 'Software Engineers Discovering How GDPR Limits the Use of Blockchain', Eweek, 11 June 2018; and 'Will GDPR Compliance Kill Blockchain?', Stanly Johnson, 4 July 2018, both as cited in 'Blockchain and the GDPR', European Union Blockchain Observatory and Forum, 16 October 2018 – https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf - last accessed 18 February 2020.

[3] The Chief Executive Officer of the Gibraltar Regulatory Authority

2. ACKNOWLEDGEMENTS

Having referred to reports and other publications of several authoritative bodies and industry participants during the drafting of this document, the Commissioner hereby acknowledges that parts of this document reflect and incorporate the opinions of, or commentary provided by or in, the following:

1. **European Commission**

    a. 'Next Generation Internet Brochure', 18 September 2019 https://ec.europa.eu/digital-single-market/en/news/next-generation-internet-brochure

    b. 'EU-Funded Projects in Blockchain Technology', 26 August 2019 https://ec.europa.eu/digital-single-market/en/news/eu-funded-projects-blockchain-technology

    c. 'European countries join Blockchain Partnership', 10 April 2018 https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership

    d. Blockchain Factsheet https://ec.europa.eu/digital-single-market/en/news/how-can-europe-benefit-blockchain-technologies

2. **European Parliament**

    a. 'Report on Blockchain: a Forward-Looking Trade Policy' (AB-0407/2018), 27 November 2018 http://www.europarl.europa.eu/doceo/document/A-8-2018-0407_EN.html

3. **European Union Blockchain Observatory and Forum**

    a. 'Blockchain and the GDPR', 16 October 2018 https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf

    b. 'Software Engineers Discovering How GDPR Limits the Use of Blockchain', Eweek, 11 June 2018; and 'Will GDPR Compliance Kill Blockchain?', Stanly Johnson, 4 July 2018, both as cited in 'Blockchain and the GDPR', 16 October 2018 https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf

    c. 'Legal and Regulatory Framework of Blockchains and Smart Contracts - Blockchain Technology and the Law', v1.0 27 September 2019 https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf.

    d. 'Workshop Report - GDPR', 8 June 2018 https://www.eublockchainforum.eu/sites/default/files/reports/workshop_2_report_-_gdpr.pdf

e. 'Blockchain Innovation in Europe', v1.1 21 August 2018 https://www.eublockchainforum.eu/sites/default/files/reports/20180727_report_innovation_in_europe_light.pdf

4. European Parliamentary Research Service, Panel for the Future of Science and Technology

a. 'Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?', July 2019 https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf

5. Article 29 Working Party (predecessor to the European Data Protection Board)

a. WP 216: Opinion 05/2014 on Anonymisation Techniques (adopted 10 April 2014) https://www.pdpjournals.com/docs/88197.pdf

6. French Commission Nationale Informatique and Liberté ("CNIL")

a. 'Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data', 6 November 2018 https://www.cnil.fr/fr/blockchain-et-rgpd-quelles-solutions-pour-un-usage-responsable-en-presence-de-donnees-personnelles

7. Lokke Moerel and Marijn Storm

a. 'Why Blockchain is not inherently at odds with GDPR', A blog summary taken from a full publication of Lokke Moerel published in European Review of Private Law 6-2019 [825-852] and in The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms (September 2019) http://documents.jdsupra.com/5fae1121-6360-40c2-847b-ece7026abcb1.pdf

3. GLOSSARY OF TERMS

Hash/Hashing	Hashing refers to the process of using an algorithm to transform data of any size into a unique fixed sized output (e.g., combination of numbers). A piece of information (e.g., a name) is run through an equation that creates a unique string of characters. Anytime the exact same name is run through the equation, the same unique string of characters will be created. If a different name (or even the same name spelled differently) is run through the equation, an entirely different string of characters will emerge.
Miner	Validates transactions before they are added to the blockchain.
Node	A computer that runs specific software which allows it to process and communicate information to other nodes. In blockchains each node stores a local version of the distributed ledger. Distributed ledger technology relies on a network of nodes.
Participant	Enters into transactions which, once validated, are included on the blockchain.
Private key	In public key cryptography (e.g. as used in various cryptocurrencies), a private key is a sequence of random alphabetical and numerical characters linked to a Public key. Private keys are only known to the Participant and are used to decrypt data on the blockchain and, in effect, sign off transactions. Private keys are analogous to passwords relating to an email address i.e. they allow access but are unable to be deciphered merely by having the email address.
Public key	In public key cryptography (e.g. as used in various cryptocurrencies), a public key is a sequence of random alphabetical and numerical characters linked to a Private key. Public keys are open to anyone in the system and are used to encrypt data. Public keys are analogous to email addresses, which require a corresponding password (private key) to gain access.
Smart contract	Pieces of code stored on a blockchain that will self-execute once deployed.
Transactional data	Information regarding the value of the transfer, address of the receiver and data payload.
Permissioned blockchain	Blockchain that is private and has controlled access via a private network or a VPN.
Permissionless blockchain	Blockchain that is open and publicly accessible.

4. WHAT IS BLOCKCHAIN?

Blockchain is a decentralised system, which allows for the collection, storage and processing of data using distributed ledger technology (also known as DLT). This type of technology is able to facilitate transactions whilst eliminating the need for a centralised operator. Although this could be considered as eliminating the need for **all** intermediaries, this is not strictly correct, as will be discussed in subsequent paragraphs.

As demonstrated by Figure 1 below, in contrast to a centralised and simple decentralised system, in a distributed ledger system those transacting do so on a peer-to-peer basis rather than by transacting with a central operator or intermediary.

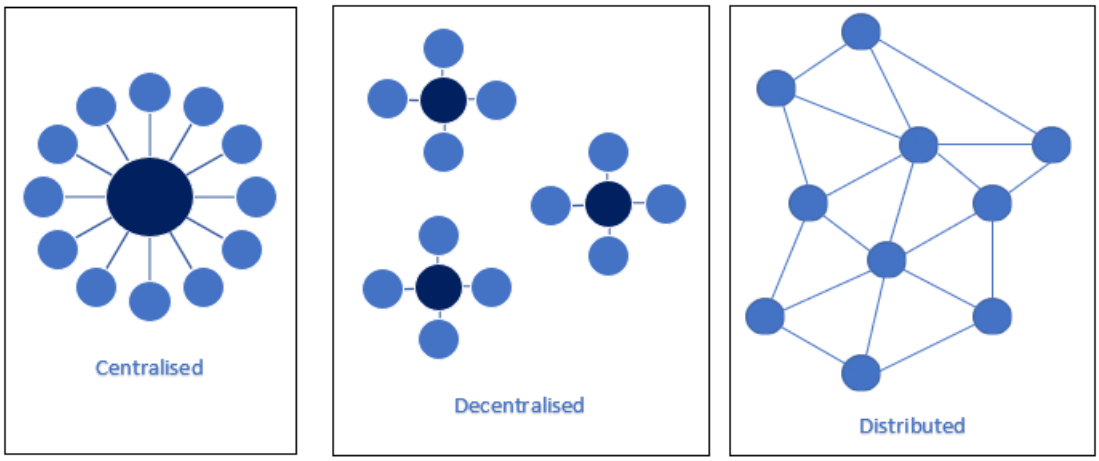

Figure 1

When a transaction is made using distributed ledger technology, the data relating to that transaction is stored in a group, or 'block'. This 'block' is then sent to various nodes within the network, where the data is validated, a process known as 'mining'. Once 'miners' ensure the transaction and data are accurate, they add the block to the blockchain. Miners could in this sense be considered a new form of intermediary (although, as seen below, debate remains with regards their position and responsibilities in respect of the GDPR).

Transactional history is indefinitely stored within the blockchain, and therefore, the data from the latest transaction is added to a chain of growing and arguably immutably stored data[4]. As ledgers within the distributed nodes share identical copies of the blockchain, it is argued that, once stored, records cannot be tampered with without leaving any trace (however, technically, and only in the most extreme circumstances, collusion involving an extensive number of nodes may potentially allow for undetected tampering).

Figure 2 below demonstrates the process whereby a new 'block' is added to the blockchain.

[4] 'Blockchain and the GDPR: Blockchain Terminology', European Union Blockchain Observatory and Forum, 16 October 2018 – https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf - last accessed 18 February 2020.

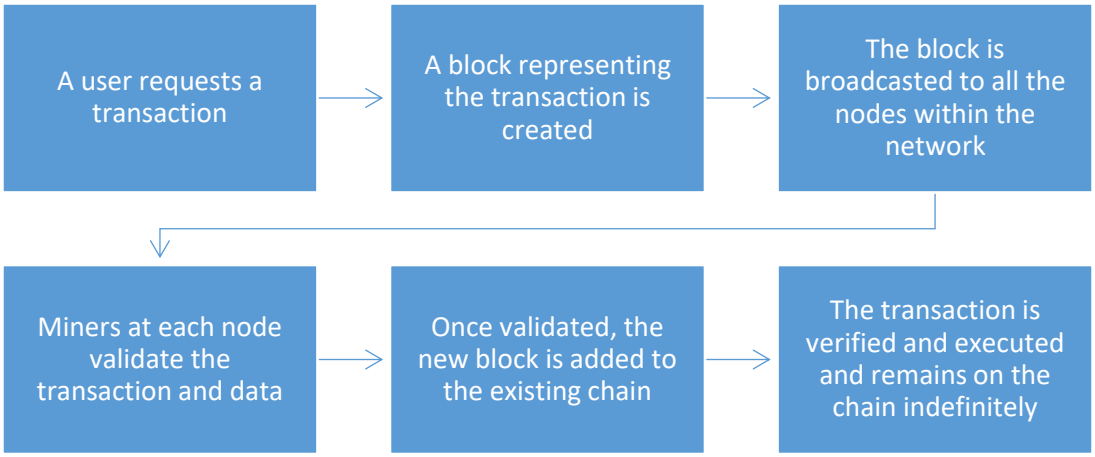

Figure 2

Importantly, although the above provides a general overview of blockchain technology and how it aims to operate, it must be recognised that blockchains are a class of technology and there is not simply one version of this technology. Consideration should therefore be given to blockchains and their usage on a case by case basis[5].

[5] 'Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law? – Blockchain Technology', European Parliamentary Research Service, Panel for the Future of Science and Technology, July 2019 - https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf – last accessed 18 February 2020.

5. INTERPLAY BETWEEN THE GDPR AND BLOCKCHAIN

With an indisputable potential to encourage economic growth and benefit transactional processes, blockchain also brings about a new paradigm of data storage and governance, leaving many unanswered questions in relation to data protection[6].

When considering the interaction between blockchain and the GDPR, it is important to firstly remember that **the GDPR places an obligation on those processing personal data, rather than on infrastructure such as blockchain technology itself**. This does not mean that those using or providing the infrastructure may not be seen to be processing personal data, but that the position must be established on a case by case basis in respect of the manner of usage of the technology, and not simply in respect of the technology itself. It is therefore imperative that the controllers and processors of personal data ensure adequate measures are in place, and that they instil a culture of privacy by design and default within their processing operations when using blockchain (or otherwise).

Personal and household exemption

It must also be noted that any natural person who enters personal data onto a blockchain for reasons unrelated to commercial or professional activity, e.g. buying or selling cryptocurrency for personal reasons, may be exempted from compliance with the GDPR by the 'personal and household exemption'[7]. In regard to blockchain therefore, a participant would be considered a data controller when they are a natural person and the processing is related to a professional or commercial activity, or, if the participant is a legal entity that registers personal data on the blockchain, for example financial institutions entering personal data relating to their customers.

Blockchain and personal data

Understanding the extent of personal data that may potentially be involved in a blockchain transaction is also of utmost importance. In this respect, both transactional data, as well as public keys[8], could fall within the GDPR's definition of personal data, namely *"any information relating to an identified or identifiable natural person"*[9]. Notwithstanding, there remains debate as to what constitutes personal data from a blockchain perspective, with some commentators suggesting that, where the provider has no access to the private key, the data should not be considered their personal data[10] . This is a matter which is the subject of debate.

[6] 'Blockchain and the GDPR: Revolution From below: Blockchain and the tools of decentralisation', European Union Blockchain Observatory and Forum, 16 October 2018 – https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf - last accessed 18 February 2020.

[7] Article 2(c) of the GDPR.

[8] Note that although the public key is broadcasted to all participants within a network, the private key is kept secret and secure.

[9] Article 4(1) of the GDPR.

[10] 'Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law? – Blockchain Technology', European Parliamentary Research Service, Panel for the Future of Science and Technology, July 2019 - https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf – last accessed 18 February 2020.

With regard transactional data, personal data could include information a participant submits when entering into a transaction which is to be added to a blockchain. Personal data may also derive from information corporate entities retain in relation to their customers, including for example their preferences, details about their purchases, or their habitual payment methods. As for public keys, these consist of an alphanumeric sequence of characters, which serve as the participant's account identifier, and can therefore be considered the participant's personal data if relating to a natural person. This is especially so when the public key is linked to additional identifiers that can disclose the relevant individual.

The increasingly wide-reaching scope of blockchain technology and the development of its use not only within a purely commercial context but also within transactions linked to individuals' daily lives, enhance the importance of the compliance and compatibility of blockchain with the GDPR.

Importantly, it must be remembered that many of the issues remain under discussion without any authoritative resolutions/conclusions. The below therefore represents a cross-section of current discussions, although aiming to highlight the most prominent issues.

6. POTENTIAL TENSIONS BETWEEN THE GDPR AND BLOCKCHAIN

The following are three areas where there may be difficulties in regard to data protection when using blockchain –

1. identifying the data controller (and often also the processor);
2. the anonymisation of personal data; and
3. the exercise of individuals' rights[11] and legal bases.

The following paragraphs must however be viewed in the context that, as explained above, there is no contradiction in principle between blockchain and the GDPR, with many blockchain-based applications conforming to GDPR standards[12]. Issues may arise depending on the distinct usages of blockchain.

A. WHO IS THE DATA CONTROLLER AND PROCESSOR WITH REGARDS BLOCKCHAIN TRANSACTIONS?

The GDPR requires the identification of a data controller who will be accountable for compliance with the GDPR. However, as blockchain relies on a decentralised model, individuals and entities transact directly with each other, and there are often many contributing parties, blurring the certainty of an identifiable controller. This contrasts with the GDPR's reliance on a hierarchical structure, in which the data controller has (or joint controllers have) ultimate control over the personal data being processed[13]. Notably however, even outside of the blockchain environment, there is often doubt as to who a controller is.

Establishing controllership in a blockchain environment is arguably even more difficult, and must therefore be considered on a case by case basis, taking into consideration the means and purposes of processing, and including an understanding of the differences between different types of blockchain e.g. 'permissioned' and 'permissionless' blockchains.

[11] 'Legal and Regulatory Framework of Blockchains and Smart Contracts - Blockchain Technology and the Law', European Union Blockchain Observatory and Forum, v1.0 27 September 2019 – https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf - last accessed 18 February 2020.

[12] 'Blockchain and the GDPR : Tensions between the GDPR and blockchain', European Union Blockchain Observatory and Forum, 16 October 2018 – https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf - last accessed 18 February 2020.

[13] 'Workshop Report - GDPR', 8 June 2018, European Union Blockchain Observatory and Forum - https://www.eublockchainforum.eu/sites/default/files/reports/workshop_2_report_-_gdpr.pdf - last accessed 18 February 2020.

In relation to a 'permissioned' blockchain, it can be argued that the participant entering into the transaction is themselves the data controller given that they submit the respective data and determine the purpose and means of the processing[14]. In respect of permissioned blockchains that are established by a consortium, it may also be the case that the consortium members are to be classified as joint controllers. This determination would depend on the particular circumstances and the level of control and decision-making by each member with regards personal data processed.

When dealing with 'permissionless' blockchain networks, it is much more difficult to identify the data controller, as these are open networks and are predominantly widely distributed. All nodes have access to all data and the blockchains are available for use by the general public for any purpose. Greater care should be taken in this context with each case requiring specific consideration.

Importantly, when establishing the data controller in circumstances where there are several participants processing personal data with the same purpose, more than one of which may fall within the potential definition of a data controller, then the data controller should ideally be identified prior to the transaction, either by appointing a legal representative, or by contractually appointing one of the participants. Failure to appoint a specific controller may, in accordance with Article 26 of the GDPR, result in all participants being considered joint controllers.[15]

Additionally, because all blockchain transactions require validation by miners, miners are potentially receiving personal data of participants. Miners who simply validate transactions sent by participants, but do not have control over what is contained within such transactions, would not generally be considered controllers[16]. However, in the event that they make any decisions on the personal data and how it is processed, they would then become a controller, or perhaps a joint controller. The same concept would apply to algorithm developers in respect of smart contracts as well as blockchain protocol developers. In this respect, core developers are sometimes co-founders and in such circumstances their responsibilities may be viewed more widely. On the other hand, a core developer may partially or completely lose their influence over the further functioning and development of a given project even though they deployed the initial software[17].

Although developers and software engineers typically do not process any personal data and may even have difficulties in foreseeing all possible deployments of their technology, in the ECJ case of Google Spain the idea of controllership was interpreted so widely so as to find that Google was a controller in respect of personal data on third party web pages. Some consider this finding to be somewhat controversial as when a website owner uses the internet to offer its website, it would typically be the view that the website owner qualifies as the controller and not the operator of the technical

[14] 'Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data', French Commission Nationale Informatique and Liberté ("CNIL"), 6 November 2018 - https://www.cnil.fr/fr/blockchain-et-rgpd-quelles-solutions-pour-un-usage-responsable-en-presence-de-donnees-personnelles - last accessed 27 January 2020.

[15] 'Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data', CNIL, 6 November 2018 - https://www.cnil.fr/fr/blockchain-et-rgpd-quelles-solutions-pour-un-usage-responsable-en-presence-de-donnees-personnelles - last accessed 27 January 2020.

[16] Ibid.

[17] 'Legal and Regulatory Framework of Blockchains and Smart Contracts - Blockchain Technology and the Law', European Union Blockchain Observatory and Forum, v1.0 27 September 2019 – https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf - last accessed 18 February 2020.

infrastructure. The debate as to the position with regards controllership of infrastructure providers therefore remains open and subject to further deliberation.

Linked to the debate on controllership, is the practicality of implementing Article 28 of the GDPR, which governs the relationship between processors and controllers, and establishes the role of processors.

In respect of miners for example, if they are to be considered processors, the potential expanse and volume of miners in a 'permissionless' blockchain creates an additional obstacle when looking to ensure adherence with the obligations under Article 28 of the GDPR. Looking to implement contractual arrangements between a controller and all miners who are deemed to be processors may be physically extremely demanding and arguably impractical. Additionally, even if it were possible to approach the owners of individual nodes with a request to enter into a contract, due to the nature of blockchain and the number of participating nodes, permanently deleting information from all nodes would be highly unlikely in the event of a request to edit or delete data.

Additionally, it has been suggested that participants themselves may be a controller with regards the data they submit, but also processors due to their storage of the entire transactional history on the blockchain[18]. Again, this could cause practical difficulties in ensuring compliance with Article 28 requirements for written agreements between controllers and processors as the number of processors may be extensive when considered in such a broad light.

B. CAN PERSONAL DATA ON A BLOCKCHAIN EVER BE ANOYMISED UNDER THE GDPR?

The GDPR applies to all personal data, defined as "*any information relating to an identified or identifiable natural person*"[19] unless it has been anonymised. In the classification of data as anonymous, it must be impossible to identify a natural person through "*all the means reasonably likely to be used*"[20].

When added to the blockchain, personal data can be entered in plain text, using encryption, or applying cryptographic security techniques such as hashing. Due to the irreversible nature of data entered onto a blockchain, i.e. once data is added it cannot be altered or removed[21], it is not recommended that personal data be stored on a blockchain in an unencrypted format. When considering encryption techniques to

[18] 'Report on Blockchain: a Forward-Looking Trade Policy' (AB-0407/2018) para 22, 27 November 2018, European Parliament, - http://www.europarl.europa.eu/doceo/document/A-8-2018-0407_EN.html - last accessed 18 February 2020.

[19] Article 4(1) of the GDPR.

[20] Recital 26 of the GDPR.

[21] There is argument that there is a possibility for data on a blockchain to be altered. However, the possibilities for alteration or removal are currently extremely slim and commercially unavailable, and information on a blockchain is therefore typically considered immutable and irreversible.

apply, there are however two main risks that must be considered; the reversibility risk, and the linkability risk.[22]

In respect of the reversibility risk, brute force attacks could reverse the encryption technique and reveal the original data set. As for the linkability risk, if each time a user makes a transaction the hash is the same, pattern analysis could make it possible to uncover the underlying information.

The debate as to what it takes to fully anonymise personal data to such a standard whereby it can be stored on the blockchain whilst remaining anonymous remains open. For example, it has not yet been concluded by any relevant authorities that hashing can be considered a sufficient form of anonymisation of data in all circumstances[23]. On the contrary, the Article 29 Working Party[24] noted that although hashing *"reduces the linkability of a dataset with the original identity of a data subject"* and thus *"is a useful security measure,"* it is *"not a method of anonymization"*[25]. This is because, although methods exist to reduce the risks associated with brute force attacks, there remains potential for the hash to be deciphered through such attacks.

Any techniques that do not meet the standard required for the data to be considered anonymised, would render the data pseudonymous instead, and, in consequence, such data would be subject to the requirements of the GDPR.

C. DATA SUBJECT GDPR RIGHTS AND LEGAL BASES

When considering the relationship between blockchain technology and the rights afforded to individuals by the GDPR, there is potential for tension and grey areas remain. The below provides a non-exhaustive list of areas where difficulties may arise:

Article 5 – Potential tensions exist in relation to the following data protection principles:

(i) Data minimisation[26]: the ongoing dissemination and replication of data is arguably inconsistent with the principle of data minimisation.

(ii) Purpose limitation[27]: due to the constant growth of the blockchain, there is a significant risk of "function creep"[28].

[22] 'Blockchain and the GDPR: Tensions between the GDPR and Blockchain', European Union Blockchain Observatory and Forum, 16 October 2018 – https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf - last accessed 18 February 2020.

[23] Ibid.

[24] The Article 29 Working Party was the predecessor to the European Data Protection Board.

[25] Article 29 Working Party, WP 216: Opinion 05/2014 on Anonymisation Techniques at 20 (adopted 10 April 2014) - https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf - last accessed 18 February 2020.

[26] Article 5(1)(c) of the GDPR.

[27] Article 5(1)(b) of the GDPR.

[28] 'Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?: Blockchain Technology', European Parliamentary Research Service, Panel for the Future of Science and Technology, July 2019 - https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf – last accessed 18 February 2020.

(iii) Storage limitation[29]: blockchain was designed for indefinite storage with the idea that each transaction would remain on the ledger for as long it was used[30].

Article 6 - Article 6 of the GDPR states that personal data can only be processed if one of the six legal bases applies. One of these legal bases is consent[31]. It could be argued that by choosing to transact on a 'permissionless' blockchain, participants are providing the requisite consent. Nevertheless, without identifying a controller, this could still be considered a passive act, and consequently remains a grey area.[32] Further, for consent to be valid an individual must be able to withdraw consent at any time[33], which is difficult given the immutability of the blockchain.

Other legal bases such as "contractual grounds"[34] are also available, however as above difficulties may arise where a data controller cannot be identified as the parties to the contract cannot be established.

Article 15 - Article 15 of the GDPR stipulates that a data subject has a right to request information from the data controller on how their personal data is being processed. However, if it is not possible to identify the data controller, the individual has no point of contact and may be unable to exercise this right. Additionally, the blockchain may have become so extensive that the exact means and purposes of processing may have changed and may even have become unknown to those initially involved in the processing.

Articles 16 and 17 - The inability to amend previous blocks within a blockchain (or at least not with any ease, due to this being one of the intended outcomes of blockchain) also raise potential issues in relation to individuals wishing to exercise their right to rectification or to erasure as provided for under Articles 16 and 17 of the GDPR. Even if the specific transaction could be located, blockchains have been deliberately designed to secure data integrity and create trust in the network, aiming to achieve this by ensuring that transactions are never forgotten and can never be amended[35]. It is however possible to include a new block within the chain with amended details where there is a concern with regards accuracy.

Additionally, in respect of erasure, it is arguably possible to make the data practically inaccessible through the use of encryption methods, which could be considered as a significant move towards the effects of data erasure. For example, if a hash function's secret key is deleted, proving or verifying which information has been hashed would no longer be possible and there would no longer be a threat to confidentiality. The

[29] Article 5(1)(h) of the GDPR.

[30] 'Blockchain and the GDPR: Tensions between the GDPR and Blockchain', European Union Blockchain Observatory and Forum, 16 October 2018 – https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf - last accessed 18 February 2020.

[31] Article 6(1)(a) of the GDPR.

[32] 'Blockchain and the GDPR: Tensions between the GDPR and Blockchain', European Union Blockchain Observatory and Forum, 16 October 2018 – https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf - last accessed 18 February 2020.

[33] Article 7(3) of the GDPR.

[34] Article 6(1)(b) of the GDPR.

[35] 'Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?: The tension between blockchain and the GDPR', European Parliamentary Research Service, Panel for the Future of Science and Technology, July 2019 - https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf – last accessed 18 February 2020.

secret key would however require deletion in all the places in which it is stored[36], which may pose another practical obstacle.

Article 19 – Further to the considerations above, it is also a requirement under Article 19 of the GDPR for a controller to communicate any rectification or erasure of personal data to other parties to which this data may have been disclosed. The question here arises as to which parties would be considered 'recipients' of the data and how this would work in practice.

Article 22 - Pursuant to Article 22 of the GDPR, individuals have the right to be informed about their data being used for automated decision making. This is directly linked for example to the use of smart contracts. Smart contracts, and blockchain in general, have been designed to automatically process information without the need for human intervention[37]. However, the use of such contracts, conflicts with the GDPR in its aims to protect individuals against legal or other significant effects arising from profiling or decision-making solely by a machine. Human intervention should be made possible to allow data subjects to contest the decision, even if the contract has already been performed[38].

[36] 'Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data', CNIL, 6 November 2018 – https://www.cnil.fr/fr/blockchain-et-rgpd-quelles-solutions-pour-un-usage-responsable-en-presence-de-donnees-personnelles. - last accessed 27 January 2020.

[37] 'Blockchain Innovation in Europe: Key challenges and barriers for blockchain in the European Union', The European Union Blockchain Observatory and Forum, v1.1 21 August 2018, https://www.eublockchainforum.eu/sites/default/files/reports/20180727_report_innovation_in_europe_light.pdf - last accessed 19 February 2020.

[38] 'Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?: Data subject rights', European Parliamentary Research Service, Panel for the Future of Science and Technology, July 2019 - https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf – last accessed 18 February 2020.

7. DATA PROTECTION OPTIONS AND OPPORTUNITIES WITH BLOCKCHAIN

Despite the potential tensions between blockchain usage and the GDPR, blockchain technology can be used in a way that is compatible with the GDPR and in some instances complementary. These are outlined in the following. However, it is important to note that these are largely subject to further debate and determination.

A. INFORMATION RIGHTS

In the foregoing risks have been identified in relation to compliance with the GDPR, including an individual's ability to exercise their rights.

An area where risks were identified concerned the right of an individual to be made aware of the processing of their personal data by a controller and for the same to be in a transparent and clear manner[39]. However, it is possible for compliant arrangements to be implemented. Provided a controller is identified, the obligations on said controller in this respect are arguably reasonably able to be actioned and should therefore not be an issue.

B. TECHNOLOGICAL DEVELPOMENTS

As a 'new technology', blockchain is evolving. This evolution can be seen as an opportunity for the technological development to be influenced early on for it to accommodate legal requirements, such as those associated with data protection.

For example, a technique known as 'pruning' is currently being developed with the aim of minimising the amount of data on the blockchain[40]. This technique aims to reduce the replication of data on the blockchain. Nodes would not require all historical transactions to verify a block but would instead go back perhaps 100 blocks (depending on the blockchain and circumstances), hence reducing the personal data it accesses. Although originally developed with the premise of improving performance, this technique could concurrently assist in blockchain's compliance with the GDPR's rights to erasure, rectification, data minimisation and storage limitation as discussed above[41].

[39] Articles 12, 13 and 14 of the GDPR.

[40] 'Blockchain and the GDPR: Opposites attract: Resolving the tensions between blockchain and the GDPR', The European Union Blockchain Observatory and Forum, 16 October 2018, https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf - last accessed 18 February 2020.

[41] Please refer to paragraph 6(c) above.

Similarly, developers are exploring the use of 'chameleon hashes'[42], which allow for the editing, removing or rewriting of data on the blockchain. In this respect, however, there is the argument that by making blockchain editable, this in effect contradicts the original concept of blockchain and its intended use, which was ultimately a technology designed to permanently record all transactions ever made in an attempt to ensure trust in the system.[43]

A 'commitment' is another cryptographic mechanism, which allows the 'freezing' of data so that it is impossible to access such data by simply using the "commit" on its own, and instead, further information is required to gain access[44].

Other advanced cryptographic techniques are also being developed in relation to blockchain, which aim to implement more robust anonymisation methods. In addition, possibilities of data aggregation techniques to anonymise personal data are also the subject of investigation[45]. Aggregation techniques such as the addition of 'noise' to the data has gained some support from the Article 29 Working Party. This technique sees several transactions being grouped together so that a third party is unable to verify the identities of the respective parties to a transaction. The Article 29 Working Party have agreed this may be an acceptable form of anonymisation, provided that necessary safeguards are complied with[46].

C. DATA GOVERNANCE AND DATA SHARING

Blockchain technologies could also be used as data governance and data sharing tools, without the need for intermediaries[47]. Transactions and direct exposure to the ledger offer a greater level of transparency and access to data subjects, thereby lending support to the GDPR's objectives in this regard. Data subjects are arguably provided with a higher level of control over their personal data, and a medium by which to themselves share data with the intended recipient when required and only when they deem appropriate to do so. Notwithstanding the benefits in respect of data sharing, it must be noted that, although blockchain can be used in the processing of data, data

[42] 'Blockchain and the GDPR – Opposites attract: Resolving the tensions between blockchain and the GDPR', The European Union Blockchain Observatory and Forum, 16 October 2018, https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf - last accessed 18 February 2020.

[43] 'Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?: The tension between blockchain and the GDPR', European Parliamentary Research Service, Panel for the Future of Science and Technology, July 2019 - https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf – last accessed 18 February 2020.

[44] 'Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data', CNIL, 6 November 2018 - https://www.cnil.fr/fr/blockchain-et-rgpd-quelles-solutions-pour-un-usage-responsable-en-presence-de-donnees-personnelles - last accessed 27 January 2020.

[45] 'Blockchain and the GDPR: Opposites attract: Resolving the tensions between blockchain and the GDPR', The European Union Blockchain Observatory and Forum, 16 October 2018, https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf - last accessed 18 February 2020.

[46] Article 29 Working Party, WP 216: Opinion 05/2014 on Anonymisation Techniques at 20 (adopted 10 April 2014) - https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf - last accessed 18 February 2020.

[47] 'Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?: Blockchains as a means to achieve GDPR objectives', European Parliamentary Research Service, Panel for the Future of Science and Technology, July 2019 - https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf – last accessed 18 February 2020.

protection is not its main priority or reason for existence, and other purposes may be seen to take priority, sometimes to the detriment of data protection principles.

D. STORAGE OF PERSONAL DATA OFF-CHAIN

Prior to the processing of personal data, it should first be considered whether blockchain technology is necessary or whether there are other suitable and more favourable options[48].

In respect to business-to-business applications there are instances in which each entity could manage the personal data of its customers 'off-chain' and use blockchain to transact other business in a faster, cheaper way, without having to publish individual transactions[49]. In effect, this could be the most compatible means of using blockchain whilst complying with the GDPR, as the data itself would not appear on the chain, whilst at the same time there would be near to immutable proof that the transaction occurred. This is sometimes referred to as 'zero knowledge proof'.

If, however, it is essential for personal data to be stored or processed on the blockchain, then, in order to heighten GDPR compliance, the processing would need to be as controlled and restricted as possible and preferably on a permissioned blockchain. The pre-determined rules of a permissioned blockchain can for example, assist in avoiding jurisdictional and enforcement disputes[50]. This is of particular importance when data is being transferred outside of the EU, as, within a permissioned blockchain, there are greater provisions for safeguards for transfers outside of the EU in comparison with 'permissionless' blockchains in which there is no control over the location of miners.[51]

Alternatively, ledger storage could be limited so that, once the data is verified and the block added to the chain, the majority of the nodes could be required to delete the data so that only a smaller number of nodes retain the same. Although this could be viewed as a compromise in respect of verifiability and trust in the blockchain, it could assist with confidentiality and data protection[52].

---

[48] "Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data", CNIL, 6 November 2018 - https://www.cnil.fr/fr/blockchain-et-rgpd-quelles-solutions-pour-un-usage-responsable-en-presence-de-donnees-personnelles - last accessed 27 January 2020

[49] 'Blockchain and the GDPR: Opposites attract: Resolving the tensions between blockchain and the GDPR', The European Union Blockchain Observatory and Forum, 16 October 2018 - https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf - last accessed 18 February 2020.

[50] 'Why Blockchain is not inherently at odds with GDPR', Lokke Moerel and Marijn Storm, A blog summary taken from a full publication of Lokke Moerel published in European Review of Private Law 6-2019 [825-852] and in The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms (September 2019) - http://documents.jdsupra.com/5fae1121-6360-40c2-847b-ece7026abcb1.pdf - last accessed 19 February 2020.

[51] 'Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data', CNIL, 6 November 2018 - https://www.cnil.fr/fr/blockchain-et-rgpd-quelles-solutions-pour-un-usage-responsable-en-presence-de-donnees-personnelles - last accessed 27 January 2020.

[52] 'Why Blockchain is not inherently at odds with GDPR', Lokke Moerel and Marijn Storm, A blog summary taken from a full publication of Lokke Moerel published in European Review of Private Law 6-2019 [825-852] and in The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms (September 2019) - http://documents.jdsupra.com/5fae1121-6360-40c2-847b-ece7026abcb1.pdf - last accessed 19 February 2020.

Importantly, in cases of high risk, a data protection impact assessment, as provided for by Article 35 of the GDPR, should be undertaken. This would need to take into consideration the particular processing and potential data subjects affected, as well as the means for the processing e.g. permissioned blockchain.

E. SECURITY CONSIDERATIONS

There are some inherent features within blockchain that could be considered positive security aspects of the technology. For example, although the above discussion noted the issues surrounding individuals' rights to rectification and erasure, having multiple copies of data may on the other hand be considered as eliminating the risks associated with potential loss from one single point of failure, as well as making unwarranted tampering a more onerous feat.

Further, in addition to the above-mentioned encryption and cryptographic techniques and the other security measures that can be seen to assist in protecting personal data within a blockchain (e.g. using permissioned blockchains, using blockchain only when required, or storing personal data off-chain), there are also other security aspects that could be taken into consideration when using blockchain for the processing of personal data. The following are some examples[53] of approaches that could be adopted:

- use of permissioned blockchains which require the least number of miners whilst still ensuring the absence of a coalition that could have excessive power over the chain;
- setting out technical and organisational procedures in advance, including procedures to combat any vulnerabilities that may arise;
- having appropriate and documented governance procedures to ensure alignment between policy and practical implementation;
- ensuring the security of keys, by for example storing them on secure media;
- using one-time public keys where possible so that new keys would be generated for each transaction.

The above are a mere fraction of the multitude of security and operational measures that could be implemented with the aim of enhancing the security of personal data on a blockchain.

[53] 'Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data', CNIL, 6 November 2018 - https://www.cnil.fr/fr/blockchain-et-rgpd-quelles-solutions-pour-un-usage-responsable-en-presence-de-donnees-personnelles - last accessed 27 January 2020.

8. REGULATORY GUIDANCE AND SUPPORT

The development and long-term survival of emerging technologies can benefit from strong legal and regulatory frameworks as part of their support system.

Recognising the potential for blockchain technology to assist in aspects of data protection, whilst also remaining conscious of the implications and risks the technology imposes on data protection, is vital when considering the path of regulatory guidance in this area. It is also important to recognise that aspects which may be beneficial from a data protection perspective (e.g. anonymisation) may not be viewed in the same light by those looking to enforce AML/CTF or other policy, legal or regulatory requirements.

Within the EU, there is however a lot of support for the growth of new technologies, as seen when issues, similar to those now faced by blockchain, arose with the arrival of cloud computing[54].

In the absence of conclusive court decisions, regulatory guidance is useful to provide greater legal certainty.

Since 2017, the EU has supported blockchain pilot projects through 'Horizon 2020' and has invested heavily in areas such as digital identity, e-health and energy[55]. Further, in respect of building a secure blockchain infrastructure, the European Blockchain Partnership was established in 2018 and holds monthly meetings in order to create a trusted environment between EU Member States and EEA countries by which to provide cross-border digital public services[56].

These initiatives, as well as other initiatives introduced by the EU Commission[57], can be considered a positive step towards narrowing the gap between blockchain usage and GDPR compliance, and even a welcome step in enhancing the benefits of them both.

Furthermore, certification mechanisms and codes of conduct may also be considered as valuable in this area. These could be progressed and agreed between regulators and players within industry, in order so that both may gain a more in-depth understanding, which may in turn be beneficial in leading to more practical approaches. This was achieved in relation to cloud computing for example[58].

---

[54] 'Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?: Support codes of conduct and certification mechanisms', European Parliamentary Research Service, Panel for the Future of Science and Technology, July 2019 - https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf – last accessed 18 February 2020.

[55] 'EU-Funded Projects in Blockchain Technology', European Commission, 26 August 2019 - https://ec.europa.eu/digital-single-market/en/news/eu-funded-projects-blockchain-technology - last accessed 19 February 2020.

[56] 'European countries join Blockchain Partnership', European Commission, 10 April 2018 - https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership - last accessed 19 February 2020.

[57] European Commission Blockchain Factsheet - https://ec.europa.eu/digital-single-market/en/news/how-can-europe-benefit-blockchain-technologies - last accessed 28th January 2020.

[58] 'Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?: Support codes of conduct and certification mechanisms', European Parliamentary Research Service, Panel for the Future of Science and Technology,

9. FINAL REMARKS

Blockchain is still an evolving technology, and, as its usage continues to evolve, many questions remain unanswered. In regard to its compatibility with the GDPR, there appears to be a trend towards developing mechanisms which may assist in improving compliance with the GDPR and reconciling both ideals.

Importantly, it is not blockchain technology itself that may lack compliance, but rather its usage[59]. The potential for GDPR requirements to be built into the technology are an opportunity for ensuring general compliance with the GDPR but in particular the principle of data protection by design and default[60].

Whilst there is the potential for data protection difficulties to arise in regard to the use of blockchain, the GDPR does not necessarily prohibit use of the technology and stakeholders must work towards finding appropriate data protection compliant solutions. The Commissioner's office will seek to engage with stakeholders in his efforts to obtain an appropriate understanding and insight into the issues/challenges faced by data controllers and provide assistance.

IMPORTANT NOTE

This document is purely for the purposes of engagement and consultation with relevant stakeholders. The document does not constitute legal advice or legal analysis. All organisations that process personal data need to be aware that the GDPR and the DPA will apply directly to them. The responsibility to become familiar with the GDPR and the DPA and comply with its provisions lies with the organisation.

July 2019 - https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf – last accessed 18 February 2020.

[59] 'Blockchain and the GDPR: Executive Summary', The European Union Blockchain Observatory and Forum, 16 October 2018, https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf - last accessed 18 February 2020.

[60] 'Blockchain and the GDPR: Tensions between blockchain and the GDPR', The European Union Blockchain Observatory and Forum, 16 October 2018, https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf - last accessed 18 February 2020.

CONTACT US

Gibraltar Regulatory Authority
2nd floor, Eurotowers 4, 1 Europort Road, Gibraltar

(+350) 20074636
privacy@gra.gi
www.gra.gi