BAI
BLOCKCHAIN ASSOCIATION
OF IRELAND

Privacy-Friendly Blockchain Technology: An Overview of Blockchain Technology and the 'GDPR'

THE BLOCKCHAIN ASSOCIATION OF IRELAND

Tanya Moeller, Simon Schwerin (Authors)

INTRODUCTION

This report is the end product of the work of the Working Group on the GDPR and Blockchain of the Blockchain Association of Ireland (hereinafter 'BAI').

TARGET AUDIENCE

The target audience of this Report is anybody with an interest in blockchain technology, law, compliance, and data protection, specifically Regulations (EU) 2016/679, commonly referred to as General Data Protection Regulations (hereinafter 'GDPR').

OBJECTIVE

The objective of this Report is to look at the interaction between emerging blockchain technologies on the one hand, and the compliance framework on the other, specifically the data protection compliance framework.

Against this context, this Report also wishes to draw attention to what the authors perceive as the necessity for blockchain technology enthusiasts to be mindful of the GDPR requirement to implement projects and new tools only on the basis of "privacy by design" in all cases where the GDPR applies. In expansive and expensive projects involving Blockchain technology, this is a key consideration for project innovation and implementation.

In this regard, we wish to cite the European Data Protection Supervisor in stating that:

"It is essential that data protection experts begin to examine the concepts behind blockchain technology and how it is implemented in order to better understand how data protection principles can be applied to it. An integral part of this process should be the development of a privacy-friendly blockchain technology, based on the principles of privacy by design. With the aim of encouraging this approach, the EDPS participated in several events on bitcoin and blockchain in 2016, and we will continue to monitor the data protection implications of blockchain technology in the year to come."[1]

METHODOLOGY

The Working Group was initially set up by Tanya Moeller, one of the authors of the Report and a main contributor to the content of the Report. Her initiative was supported by the BAI but the findings of the working group are independent from the BAI. The findings of the Report, although copyrighted to the authors and the BAI jointly, are the opinions of the active members of the Working Group, which are as follows:[2]

- Tanya Moeller (author and contributor)
- Simon Schwerin (author and contributor)
- Grant Leech (contributor)
- Niall Clancy (contributor)
- Patrick Cryan (contributor)
- Sri Durga Meghana Yadav (contributor)

[1] https://edps.europa.eu/sites/edp/files/publication/17-04-27_annual_report_2016_en_1.pdf, para 4.5.4.

[2] The authors of this Report would also like to thank those members of the Working Group and indeed the BAI who have contributed to this Report, but who have not joined the Working Group as long-term active participants nor wished to be named as contributors to the content of this Report.

Content was created through face-to-face discussions, conference calls, written electronic communications and drafting this Report. The findings of this Report are the result of approximately four months of work. Key decisions were taken on a democratic basis.

The contributors of the Working Group were split into the following three groups: firstly, persons with a predominant background and interest in Computer Science and technology; secondly, persons with a predominant background in law and data protection and thirdly, persons with a predominant background or interest in both these areas. Members of each of those groups were requested to check the contributions of other members for accuracy, as it was felt amongst the Working Group that this would produce the highest level of accuracy possible.

EXECUTIVE SUMMARY

Blockchain technology can be best described a technology which is in its genesis phase. It is actively growing and changing on a global scale by the many varied contributors worldwide.

When looked at through the lens of compliance, blockchain technology could therefore best be described as a 'moving target'. This makes the findings of this Report a matter of complexity as it is desirable to be specific, yet the ongoing development of the subject-matter increases the risk that everything but high level findings will rapidly fade in terms of relevance.

Furthermore, given the lack of international focus on the interaction between blockchain technology, on the one hand, and compliance areas such as data protection, on the other, there are few authoritative sources on the subject, which this Report can draw on.

Repeatedly, the Authors of this Report felt that they were exploring novel territory.

As a result, a conclusion was drawn that this Report would remain on a high level to act as a type of kick-starter for generating debate on a European, and possibly international level, on this subject matter.

In our view, there exist fundamental difficulties with the compliance of blockchain technology in the framework of the GDPR when considering that its essential features, such as its immutability and incorruptibility, are also some of its greatest stumbling blocks in terms of vindicating the data subject's rights.

This Report provides at its heart a key sequence of questions which will hopefully assist the wider community in assessing their own blockchain technology based projects in terms of GDPR compliance.

KEY DEFINITIONS

This Report uses legal terms as defined by the GDPR[3]:

- 'Personal data' means 'any information relating to a data subject';
- A 'Data Subject' is defined as 'an identifiable natural person is one who can be identified, directly or indirectly, 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 natural person';

[3] Article 4 of the GDPR.

- A 'Data Controller' means 'the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law';

- A 'Data Processor' means 'a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller';

- 'Processing' means 'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction';

- 'Pseudo-anonymised' means 'the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person';

- 'Special categories of data' are defined as 'processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited';

- ‘Consent’ of the data subject means ‘any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her’.

This Report also uses the following technical definition:

- Blockchain technology: We are adopting this term as explained in the online blog post, “Gentle Introduction”, which describes blockchain technology as “distributed ledgers, i.e. a list of transactions that is replicated across a number of computers, rather than being stored on a central server”. The distinction between a blockchain technology and another type of database is that “a blockchain system is a package which contains a normal database plus some software that adds new rows, validates that new rows conform to pre-agreed rules, and listens and broadcasts new rows to its peers across a network, ensuring that all peers have the same data in their databases”. A blockchain “is just a file”, a type of “data structure”, in other words, “how data is logically put together and stored.”[4] As such, its interaction with data protection legislation is immediately of interest.

KEY PRESUMPTIONS

The GDPR applies only in certain circumstances. In order for the GDPR to be relevant to blockchain technology, it must process personal data in certain circumstances. For the purpose of this Report it is assumed as follows:-

[4] “A Gentle Introduction to Blockchain”, https://bitsonblocks.net/2015/09/09/a-gentle-introduction-to-blockchain-technology.

- The data being processed is not anonymous, but is personal data and therefore allow for the personal identification of the Data Subject in one form or another (through lack of anonymisation or pseudonymisation[5]);
- The data is personal data or a special category of personal data as defined by the GDPR;
- The data is processed in such territorial or other operational circumstances that the GDPR applies (the GDPR provides provisions concerning territorial scope and general application)[6];
- The data is processed after the GDPR becomes effective (after the 25th May 2018)[7];
- Relevant key parties are identifiable:
    - A Data Subject, who can be identified using the data in question;
    - A Data Controller, who controls the collection of the data from the Data Subject and who can decide and oversee the processing activity using blockchain technology.[8]

[5] Recital 23 of the GDPR.

[6] Articles 2 and 3 of the GDPR.

[7] Article 99 of the GDPR.

[8] A Data Processor may exist, but is not strictly speaking necessary as data processing can take place in-house within the Data Controller's remit.

It is acknowledged that blockchain technology can work, for example as a virtual currency platform, in a manner where a Data Controller and possibly a corresponding Data Processor is difficult to identify.

It is outside the remit of this Report to draw a distinction between, one the one hand, a private blockchain technology, where the ledger is controlled by one or several predetermined legal entities, and a public blockchain technology, on the other hand, which acts on the basis of predetermined rules and set democratic decision-making systems (such as the Bitcoin blockchain currency platform). The Authors wish to acknowledge that another analysis, which would draw such a distinction, should be done at another time and in another forum, in the future.[9]

KEY PROVISIONS

In essence, the GDPR puts conditions on the processing of personal data. Although this Report shall not give an in-depth analysis of the GDPR, the following examples can give a flavour of the complex obligations placed upon parties involved in the processing of personal data, in order to be compliant.

Article 5(a) of the GDPR provides that personal data is processed "lawfully, fairly and in a transparent manner in relation to the data subject" and the GDPR prescribes, in various mechanisms, what this requirement means in practice. Certain information must be given to the data subject.[10]

Further, personal data must only be collected if it is done for "specified, explicit and legitimate purposes" and, crucially, it cannot be further processed in a way which is

[9] For more information about public and private blockchains, see "A Gentle Introduction to Blockchain", idem.

[10] Article 14 of the GDPR.

"incompatible with those purposes".[11] As such, a never-ending processing activity of personal data for loosely defined reasons should not occur.

The GDPR also provides that personal data is only processed if it is "adequate, relevant and limited to the minimum necessary in relation to the purposes for which they are processed", in other words, personal data should not be processed if exceeds the minimum requirements. Other, alternative means of processing should be preferred if they involve data, which is not 'personal data'.[12]

Crucially for blockchain technology, the personal data in question must be "accurate and kept up to date", which means that "every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay".[13] The requirement of having a facility to erase echoes the data subject's right to be forgotten, which is provided in Article 17 of the GDPR.

Equally, the GDPR calls for technological and other measures which "permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed" and there are restrictions on storage of personal data.[14]

[11] Article 5 (b) of the GDPR.

[12] Article 5 (c) of the GDPR.

[13] Article 5 (d) of the GDPR.

[14] Article 5 (e) of the GDPR.

Data subjects enjoy certain rights and freedoms, such as the right to object to processing[15] and the right to data portability[16], which may be interesting for blockchain technologies and the harmonisation of same.

Furthermore, the data subjects shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or similar.[17]

Important for blockchain technologies is that the restriction of processing of personal data in the context of transfers to third countries or an international organisation unless certain requirements are fulfilled and safeguards put in place, in order to "ensure that the level of protection of natural persons guaranteed by (the GDPR) is not undermined.[18] In this context, Supervisory Authorities supervise the data processing of the personal data.[19]

Data Protection Officers are designated,[20] privacy impact assessments need to be carried out [21] and the right of access by the data subject is granted.[22] The principle of privacy by design requires that processing of personal data is carried out in such a manner that appropriate technical and organisational measures, such as pseudonymisation, are implemented in such a

[15] Article 21 of the GDPR.

[16] Article 20 of the GDPR.

[17] Article 22 of the GDPR.

[18] Chapter 5 of the GDPR.

[19] Chapter 6 of the GDPR.

[20] Article 37 of the GDPR.

[21] Article 35 of the GDPR.

[22] Article 15 of the GDPR.

manner that the rights of the data subjects are protected and compliance with the GDPR guaranteed.[23]

Although the above are snapshots only of the rights and freedoms of the data subject, as well as the obligations of the data controller and data processors, it is hoped that this provides a useful insight into the extent to which the GDPR has an impact on the processing of personal data in a European context. As such, the persons charged with designing and implementing blockchain technologies need to be mindful of the provisions of the GDPR.

KEY QUESTIONS

In order to be legally compliant, the GDPR requires that a Data Controller thinks carefully about implementing projects which involve the processing of personal data. The following are a number of key questions, which should be considered before blockchain technology is used for processing personal data.

Preliminary Questions

These preliminary questions assist in setting the overall framework.

The parties

- Who is the data subject in this processing activity? In other words, whose personal data is involved?
- Who is the Data Controller? Is there a single Data Controller or are there joint Data Controllers?[24]

[23] Article 25 of the GDPR.

[24] For a definition of Joint Controllers, see Article 26 of the GDPR.

- Who is the Data Processor? Are there primary Data Processors, and other, secondary, Data Processors further down the processing chain?
- Are there any other parties to the processing? What is their status?
- Where are the parties? Is there transfer of data outside the EU? Are there appropriate safeguards in place in terms of transferring data?

The Processing Activity

- What type of processing will take place?
- How is the processing activity defined?
- How does the swim lane of data look like?

The Technology

- On what blockchain technology will the processing take place – what are its features?

The personal data

- What type of personal data will be processed?
- Will special categories of data be processed?

Privacy by design

- Can this processing project be carried out in such a way that data protection does not apply, considering its scope?
- Can the data and the processing be categorised in such a way that the impact of the processing activity on the data subject's freedoms is softened, to the fullest extent?

These questions assist in evaluating the processing activity, which involves blockchain technology, to a greater extent.

- Exemptions: does an exemption apply, which permits the data controller to carry out processing of data in the manner envisaged?
- Is special care paid to the processing of special categories of personal data, such as ethnicity and health data?
- Will the processing be carried out in a fair, lawful and transparent manner?
- Is the purpose for the processing sufficiently defined? Is there a danger of a secondary, more hidden purpose? What safeguards are put in place to prevent such a secondary, more hidden purpose to affect the processing in the future?
- Are there sufficient operational and technical measures in place to safeguard the data from unauthorised acts of interference, amendment, deletion or similar?
- Can the data be accurately amended and corrected in order reflect the instructions obtained from the Data Subject in this regard?
- Is the processing activity designed in such a manner that it is minimised to the greatest extent possible? Or would an independent examiner of my processing activity conclude that it is excessive and not strictly speaking necessary for the purpose which was defined at the beginning of the process?
- Can the processing be suspended for a restricted period of time pending an investigation into a complaint by a Data Subject?
- Can the data be deleted, in the context of the Data Subject's right to be forgotten?

- Is the Data Subject subject to decisions having a legal or a similar effect, which are solely based on an automated decision-making process? What safeguards are in place?
- Is the data kept within the European Union or is it transferred outside the European Union? In the latter case, do appropriate exemptions apply? Are all the necessary precautions taken?
- Is it necessary to appoint a Data Protection Officer?
- Which Supervisory Authority is responsible? How is the reporting on the blockchain technology's use carried out in a legally compliant manner?
- Can Subject Access Request of the Data Subject be entertained?

KEY CONCERNS

When looking at the above questions and using them as a guideline, it becomes clear that any natural or legal person who wishes to work with blockchain technology needs to carefully consider the legal obligations imposed by the GDPR. Key concerns arise in this regard as to how blockchain technologies can be compliant in a data protection context. For example:

- Data portability in public blockchains: How can blockchain technology be designed in such a way that the data subject can enjoy his or her right to data portability? This also applies regarding interoperability protocols and atomic swaps between blockchains.
- Smart Contracts in the context of automated decision making: How can blockchain technology be compliant with the requirements concerning

automated decisions, especially in the context of smart contracts? How do we ensure that data protection legislation is complied with when attaching legal documents to smart contracts and blockchains?

- How can the right to be forgotten be enforced? If data in the processing chain is cut off, would this go against the inherent nature of a blockchain technology? The same goes, for example, for a chameleon hash, which induces an editable blockchain, if enough members of a federation agree to the edit.[25]
- If a blockchain technology has processed personal data, at the end of the processing activity, how can personal data be anonymised or deleted so that it is no longer stored than absolutely necessary? Does the stringent application of data protection principles in fact prohibit the operation of any kind of public blockchain from storing personal data?
- Processing in regards to consensus mechanisms and mining, e.g. Proof of Work is a question. In the process of verifying a transaction, what is the status of miners?
- When talking public blockchains and forked blockchains and side-chains, how do we define the purpose for processing, when and how we do know who will fork the chain for new kind of applications?
- Can blockchain technology in the context of privacy by design be built in a way that can be accepted in the context of data protection compliance, because its immutability and incorruptibility can be used as assets rather than a hindrance?
- What is the position of so-called "wallet holders" in the GDPR landscape?

[25] https//eprint.iacr.org/2003/167.pdf.

- Who is the Data Protection Officer in the context of a blockchain technology and what would be his or her practical role in the context of applying this type of technology?
- What is the jurisdiction of the blockchain? Would the location of the Data Controller define the jurisdiction of the blockchain? This is relevant especially in the context of blockchain technology superseding international borders.
- How are GDPR-compliant processing logs created in the context of blockchain technology?
- How can the principle of privacy by design be applied to building and implementing blockchain technology in the case of dapps (decentralised applications)? What is the legal role in the data protection compliance landscape of a company, which provides a dapp when it builds its application on top of a public blockchain?

CONCLUSIONS

The GDPR is a significant piece of new legislation in the history of European data protection. Any Data Controller and, naturally, any Data Processor who processes personal data with a European Union dimension must be compliant from 25th May 2018 onwards.

The novel features of blockchain technology make it impossible to predict how regulators will assess its strengths and weaknesses. It may well be the case that its greatest beneficial features, such as immutability and transparency, will also be the greatest stumbling blocks on the path to data protection compliance and widespread usability.

Undoubtedly, blockchain technology is attractive for all types of applications where no personal data is processed. Where personal data is used, however, and as indicated earlier in this report, the authors felt very much that this would lead to an exploration of novel territory.

Certainly, the application of data protection principles on public and private blockchains requires further work.

Nevertheless, one aspect of the GDPR is certain: It calls for the implementation of the principle of privacy by design across the board of all types of processing projects. For this reason, this report would like to conclude that the words of the European Data Protection Supervisor should be carefully heeded, who called for the development of a privacy-friendly blockchain technology, based on the principles of privacy by design.

Amongst the uncertainty of it all, it is safe to assume that creating a blockchain technology, which is data protection compliant, will mitigate regulatory risk and thereby create a significant competitive advantage.