FINTECHNORTH

REPORT

Exploring the compatibility of GDPR and Blockchain

Authored by: Bird Lovegod in association with Cygnetise
Distribution Partner Fintech North

Understanding GDPR and Blockchain

The compatibility of blockchain systems with GDPR requirements is considered by comparing features of blockchain against principles of GDPR and the subsequent impact on Individual Rights.

We then offer some potential solutions for some of the compatibility issues.

Terminology:

- GDPR: The EU General Data Protection Regulation. Published in May 2016 and effective as of May 2018. Replaced the Data Protection Directive (95/46/EC). Relevant to all EU member states including UK. Relates to Personal Data only.
- Personal Data: Information relating to a living person that identifies them or makes them identifiable.
- Data Controller: The individual or organisation which determines the purposes for the data use, the manner by which it is collected and processed.
- Data Processor: The individual or organisation processing the data on behalf of the Data Controller.
- Data Subject: The individual whose data is being processed.

Disclaimer: The opinions and potential solutions are for consideration only. Anyone wishing to explore this further should take qualified independent legal advice and seek the advice of the ICO.

Principles of GDPR and the Rights of the Individuals

GDPR is based on 7 principles designed to stay relevant and applicable and not be negated by changes in technology, markets, or other environments.
SOURCE: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

The principles lie at the heart of the GDPR. They are set out right at the start of the legislation and inform everything that follows. They don't give hard and fast rules, but rather embody the spirit of the general data protection regime - and as such there are very limited exceptions. The principles are designed to stay relevant and current, acknowledging that technical and commercial progress will create scenarios unpredictable by legislators.
Compliance with the spirit of these key principles is therefore a fundamental building block for good data protection practice. It is also key to your compliance with the detailed provisions of the GPDR.
Source: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/

Understanding the principles and adhering to them in practice is of primary importance. When questioning 'what does GDPR have to say regarding this proposed activity or system' it is important to identify the principle/s which are impacted. This will inform good decision making and compliant behaviors. Understanding how the Principles relate to the Individual Rights will provide a higher level of comprehension of the GDPR requirements and will guide correct thinking and decision making in this context.

Individual Rights afforded under GDPR

The GDPR provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

Source: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

Blockchain

Having laid out the principles of GDPR, upon which the GDPR legislation rests, and the Rights of the Individuals, which the legislation serves, we can next begin to explore blockchain, and how the meeting of GDPR and blockchain impacts GDPR Principles and Individual Rights.

The initial and immediate compatibility issue arise because blockchains are decentralised ledgers. There is no central holding place of the data, nor in some instances a central authority for the system itself. The ledger of information and the means by which it is shared is distributed across the entire network. There is no data 'base'.

Principles of Blockchain

- Every computer or group of computers in the network has a copy of the ledger.
- The ledger is formatted as blocks of information.
- A new block is created at regular and frequent intervals as determined by the blockchain operating protocol.
- Each block is verified to be true by the consensus of the network.
- Once verified by the consensus of the network, the block is added to the chain.
- Once added to the chain, the block cannot be deleted.
- Once added to the chain, the information within the block cannot be changed.

'The Blockchain' is generally considered to be the sum of all the information, plus the operating system or protocol of that specific blockchain. The protocol determines how the blockchain works in practice, defining the rules of it.

Public Blockchains

Public Blockchains, such as the bitcoin blockchain, are fully decentralised. There is no central individual or organisation with the authority or ability to make claims of control or ownership. Anyone can join a public blockchain and become part of the consensus. No single individual or organisation is responsible for it.

Private Blockchains

Private blockchains use the same technology principles, however they are individually or corporately designed and operated. Permissions are required to join the network. This can include being 'invite only'. The protocol or operating system of a private blockchain can be amended by the operator.

Features of PUBLIC Blockchain and effect on GDPR Principles

By focusing on the features of blockchain rather than the technology of it we can compare those features against the principles of GDPR, and in doing so determine compatibility issues.

Decentralisation

The decentralised structure of blockchain has an immediate impact even more fundamental than challenging the GDPR Principles. The decentralised structure of blockchain challenges the actual definitions used to structure the GDPR legislation.

The first questions are 'Who is the Data Controller and Data Processor?' and therefor **'Who is accountable?'** This is problematic. There are at least three possible perceptions.

- It could be considered the 'Data Controller and Processor' are in fact the blockchain itself. It is an operating system with protocol for data control and processing integrated into its programming. If the data controller is the blockchain itself, this poses substantial problems for the ensurance of GDPR compliance. The decentralised nature of public blockchains may be seen to evade GDPR altogether, by not meeting the fundamental definitions, and in practice, being 'controlled' by no single individual or group.
- It could equally be considered the 'Data Controller and Processor' are in practice the consensus of the nodes, the computers within the network. Again, a function of the blockchain protocol. This may or may not be a sustainable argument, and in either instance is an unhelpful definition in terms of enforcement, it only having the effect of narrowing responsibility down from 'everyone' to '51% of everyone at any given time'.
- It could also be considered the 'Data Controllers and Processors' are the Data Subjects, the individuals themselves. They hold their own information, in that they hold a copy of the entire blockchain, and if the 'Data Roles' are the collective or the consensus thereof, they become 'De facto Data Controllers and Processors' when joining. This seems the most likely interpretation in a public blockchain.

Initial Conclusion Regarding Data Roles:

The first hurdle is not a trivial one, identifying who (or what) holds the roles the GDPR legislation applies to. It seems on the face of it that either:

- There is no data controller or data processor
- Or
- Everyone is a data controller and data processor

In a truly decentralised Peer to Peer system these seem to be the only two logical conclusions. It's either everyone or no one. In practice the lack of a centralised identity for the system makes the enforcement of rules practically impossible. According to the legislator's own definitions, it may be there is no one and no-thing to address, challenge, question, or prosecute. The key issue here is that the technological structure of public blockchains may negate some of the fundamental structures of GDPR.

For Consideration

GDPR and Blockchain are trying to do the same thing, protect people's privacy. One is approaching it as regulation, the other as technology. It so happens that at some points the technological solution of one conflicts with the regulatory principles of the other.

GDPR is based on a linear understanding of data collection and management, assuming a centralised system is used. Blockchain systems are alien to this, using a non linear, decentralised methodology. There is no base for the data.

In order to break the Catch 22 it may be useful to consider the impact on the Rights of the Individual, as this implies an intent to adhere to the spirit of the legislation. If a blockchain system has acted in accordance with protecting the rights of an individual, albeit through technology rather than regulation, it may be arguable they have acted within the spirit of GDPR, to their best ability.

Let us move on to Private Blockchains, and explore the issues again, in hope of a brighter future.

Features of PRIVATE Blockchain and effect on GDPR Principles

As before, by focusing on the features of blockchain rather than the technology of it we can compare those features against the principles of GDPR, and in doing so determine compatibility issues.

Decentralisation

The decentralised structure of private blockchains is far less extreme than the public ones. The ledger is distributed amongst the network, but the network itself is closed, with a much smaller number of 'nodes.' This could be as small a number as three. Therefor the decentralised structure of a private blockchain may be far more compatible with GDPR than the public ones. These private blockchains are also called 'permissioned ledgers' as permission is required to join them. Permissioning establishes a hierarchy.

Who is the Data Controller? Who is the Data Processor?

It's reasonable to make the following assertions: The 'Data Processor' is probably the initiating company or organisation that owns the blockchain. They are responsible for it. They control what it can and cannot do. Everyone who joins is a Data Controller. It may be, depending on the rights given to Data Controllers, that they are also Data Processors.

Conclusion:

- The Data Processor is the initiator and owner of the blockchain.
- The Data Controllers the parties that subsequently join the blockchain.
- In some instances, the joining parties may also become Data Processors.
- The initial Data Processor may also be a Data Controller.

This is a hugely simplified situation compared to public blockchains and falls easily within the structure and language of GDPR. It is clear who has what roles, and who is accountable. Data Role titles can be clearly assigned as part of joining agreements.
Having easily overcome the first hurdle of assignment of roles, let's move on to the single biggest incompatibility.

GDPR Principle 5 vs Blockchain Immutability

The first four GDPR Principles are not inherently problematic for private blockchain, nor are the last two. However, the sticking point is Principle 5, **Storage limitation.** Once data is stored on a blockchain it cannot be removed or changed. As a consequence there are individual rights which may be breached by a private blockchain. Specifically, the right to erasure.

How then can immutable private blockchains be designed to enable compliance with Principal 5, Limitation of Time of Storage, and uphold the Individual Rights to have data erased? This is a large question, and here we attempt to address it in brief.

Avoiding Breaching Individuals Rights to Erasure

If data in a blockchain cannot be deleted, how then can this right be upheld?

Technical solutions:

Can data be 'anonymised'? (short answer – probably not)

Anonymised data is that for which there is no way of tracing it back to the individuals. Guidance from the EU states that 'Anonymisation results from processing personal data in order to irreversibly prevent identification'. For example, the data point '75% of people surveyed had brown hair', has no way to be traced back to those 75% of people, and is therefore anonymised.

Can data be encrypted, 'pseudoanonymised'?

Here we refer to the EU Data Protection Working Party: "*Pseudonymisation reduces the linkability of a dataset with the original identity of a data subject; as such, it is a useful security measure but not a method of anonymisation*". Can Pseudonymisation by encryption serve the same function? "*Therefore the Working Party stresses that anonymisation techniques can provide privacy guarantees, but only if their application is engineered appropriately – which means that the prerequisites (context) and the objective(s) of the anonymisation process must be clearly set out in order to achieve the targeted anonymisation level*."

For a blockchain company, questions include 'are Singling out, Linkability, and Inference still a risk?' Other factors to take into account are the public or private nature of the data sharing, is it going on the internet or is it shared only with trusted parties? How sensitive is the data? How likely is it to have value for criminal purposes? What encryption methods are suitable? Can encryption keys be 'destroyed' to achieve an 'erasure equivalent'?

"*The optimal solution should be decided on a case-by-case basis, possibly by using a combination of different techniques, while taking into account the practical recommendations developed in this Opinion". Particular attention should be paid to the criteria of: "(i) is it still possible to single out an individual, (ii) is it still possible to link records relating to an individual, and (iii) can information be inferred concerning an individual?"*

For more on this see ARTICLE 29 DATA PROTECTION WORKING PARTY Opinion 05/2014 on Anonymisation Techniques. Adopted on 10 April 2014. https://www.pdpjournals.com/docs/88197.pdf

Can Hashes be rendered 'unlinkable' to individuals?

If this technical issue can be successfully addressed, effectively and permanently anonymising hashes in order to prevent 'linkability', an acceptable alternative to erasure may be outcomed. It's another layer of cryptography, a major technical challenge, and a failure in the system could render the organisation liable for failing to comply.

Can 'Offchains and Sidechains' be developed?

There are instances where blockchains are used to manage data transfer, but data records themselves are held 'off chain' in a conventional database. This however defies the point and functionality of blockchain as a decentralised system. There are experiments with creating

'sidechains', parallel chains which may have a variable degree of functionality. Again, these are unlikely to provide satisfactory outcomes in the near future. It's not practical.

A combination of technical and non-technical solutions in keeping with GDPR?
It may be the technical incompatibilities are insurmountable. However, in practice, the purpose of the legislation, and the spirit of it, may still be adhered to by the use of private blockchains. There is a potential solution. The technology cannot be changed, the GDPR principles cannot be changed, but the rights of the individual can be changed, by the individual themselves.

This methodology uses the GDPR principle of **Lawfulness, fairness and transparency** in conjunction with the **Individuals Right to be informed.** Prior to the Data Subject entering any data, the data subjects are given a clear, fair, and transparent choice, regarding how that data is controlled and processed.

Example of providing the data subject with informed choice.

'Under GDPR you have the right to request your data be erased. *We use a secure blockchain system. This means your data cannot be erased. Instead of erasure we use* ***(XYZ) encryption.*** *In keeping with the principles of GDPR and your rights as an individual do you agree to have your data securely encrypted rather than erased? Please type YES to agree…click MORE for more information or discontinue registration to decline'.*

This transparent and informative approach may be sufficient to avoid breaching the Individuals Rights whilst adhering to GDPR Principles. In effect, the individual, the data subject, is giving informed consent for an adjustment of their rights. This acknowledges that different technologies may provide variable rights by design and enables informed individuals the ability to choose technology services accordingly. This is arguably very much in line with the purpose and spirit of GDPR, to give people control over their data and the way it is used. If encryption is used rather than erasure, it must be explained clearly and transparently prior to data collection. This is in keeping with GDPR Principle 1 relating to lawfulness, transparency and fairness.

Therefore, using this methodology, providing the encryption process is thorough and designed to be irreversible, it is possible encryption may be used as a substitute for erasure *with the Data Subjects informed consent*.

The same approach may be used to address the Principle of Storage Limitation. Example:

'Under GDPR Principle 5 we are required to limit the duration of data storage. We use a secure and immutable blockchain system. This means we cannot limit the duration of your securely encrypted data. In keeping with the principles of GDPR and your rights as an individual do you agree to have your securely encrypted data stored without limit of duration? Please type YES to agree…, click MORE for more information, or discontinue registration if you decline.'

It may be this approach, and level of transparency and service, fulfills the requirement of GDPR, adheres to the spirit of the principles, and honors the individual's rights, including their ownership of data, and authority over how that data is processed. One could argue it extends the individuals rights beyond GDPR, giving the individual the right to determine their own rights. Providing the outcome is comparable, providing the data is encrypted in such a way as to make it equivalent to erasure, and providing the data subject has explicitly agreed to this, it would seem an acceptable solution to an otherwise intractable problem. It is important to note any such work arounds must be actively opted

into, by the data subject, with informed consent, and cannot be assumed. If all technical means available are used, coupled with fairness openness and transparency, it may be the 'best of both worlds' outcome is possible. The final question becomes then: **"Has an individual the right to amend their own rights?"** That being the ultimate right. Perhaps that is something for the individuals themselves to decide.

Disclaimer: The opinions and potential solutions are for consideration only. Anyone wishing to explore this further should take qualified independent legal advice and seek the advice of the ICO.

About Cygnetise

Cygnetise is a live blockchain application built to help organisations manage their authorised signatory lists in efficient and secure manner.

The key issues with managing such lists accumulate around the excessive amount of time spent creating, reviewing, updating and distributing them (every year thousands of man hours are wasted in the process). In addition, the lack of an audit trail opens up many possibilities of fraud.

Utilising DLT technology, Cygnetise enables clients to significantly increase efficiencies by removing the existing administrative burden and enhance the control of their data, all whilst retaining the same level of detail available in the current process.

Visit **cygnetise.com**

Contact **info@cygnetise.com**

About Bird Lovegod

Bird Lovegod is an independent consultant, entrepreneur, and journalist, specialising in financial technology, future technology, and ethics.

Visit **birdlovegod.com**

About FinTech North

FinTech North is a not-for-profit, collaborative project conceived and created through the partnership of White Label Crowdfunding and Whitecap Consulting.

The FinTech North initiative aims to:

- Generate collaboration and knowledge share by building a FinTech community across the Northern Powerhouse.
- Enhance reputation of the Northern Powerhouse as a FinTech region.
- Generate tangible economic benefit for the region and the cities within it.

We do this by managing a predominantly event-based FinTech entity focused on the the Northern Powerhouse – providing a platform for sharing best practice showcasing regional talent and facilitating connections. We also engage with key public and private sector organisations and higher education establishments in the region.

Visit **fintechnorth.uk**