Blockchain and the GDPR: reconcilable differences?

March 2019

A version of this article first appeared in the Privacy Laws & Business UK Report, Issue 102 (March 2019). It is an abridged version of the full paper "March of the blocks: GDPR and the blockchain", published jointly by Slaughter and May and Cravath, Swaine and Moore LLP in February 2019, as commissioned by the Center for Global Enterprise.

Summary

Blockchain technology has advanced tremendously over the past decade, and now provides a viable alternative to traditional database solutions. However, the General Data Protection Regulation (GDPR) poses significant compliance hurdles to the ongoing development of blockchain-based solutions that involve storing (and transacting with) personal data. Some have gone so far as to call blockchain fundamentally incompatible with the GDPR. However, with some collaborative, proactive and innovative thinking by lawmakers and technology providers alike (and some much needed, up-to-date guidance from European regulators) blockchain solutions that respect the fundamental principles of data protection and privacy are achievable.

A background to blockchain

PL&B published an article in its December 2017 international edition titled "Blockchain: Disrupting data protection?" which provides a helpful introduction to blockchain and distributed ledger technology. That article is recommended for anyone who has not yet come into meaningful contact with blockchain technology. Simply put, a blockchain is a series of blocks of data, linked together by a cryptographic hash. Cryptographic hashing, one of the cornerstones of blockchain technology, works by using an algorithm to turn a block of data of any length into a random fixed-length output (i.e. a "hash"). Each block of data in the blockchain includes a hash of the previous block. Because the previous block in the chain includes a hash of the block before that one (and so on back to the first block), the blocks form a continuous, unbroken chain that is decentralised, accessible and reliable.

As a result, blockchain technology is being applied to a growing range of solutions for recording, processing and sharing information.

The hash stored in each block of the chain effectively acts as a fingerprint of the previous block. A hashing algorithm can then be passed over the previous block in the chain to confirm that it generates the correct hash. If the previous block is changed in any way, it will not generate the correct hash and the chain will be broken. This is where blockchain's immutable nature originates: the data of any block in the chain cannot be modified without changing the hash of every block that follows it.

Interestingly, as businesses have developed increasingly innovative blockchain-based solutions to an increasingly broad range of problems, governments, regulators and organisations have become more active in creating meaningful

support for blockchain's huge potential. There still remains, however, significant concern about the application of the GDPR to blockchain technology, and about the difficulty of achieving a GDPR-compliant blockchain solution.

Blockchain vs. GDPR

Some of the most revolutionary features of blockchain technology, notably the generally immutable nature of data on a blockchain, do not sit neatly with key obligations under the GDPR. The most obvious difficulties stem from the GDPR's obligations to uphold data subjects' rights to erasure and rectification, which do not sit well with a technology whose most valuable property is the absolute, immutable nature of data it processes.

However, while some applications of blockchain technology (such as most public, permissionless blockchains, theoretically accessible to anyone in the world) will almost certainly end up not being compliant with the GDPR, GDPR-compliant solutions must not be viewed as being intrinsically unachievable.

Some possible solutions?

With some up-to-date and pragmatic guidance from data protection regulators, a blockchain solution that respects the fundamental principles of data protection and privacy will be achievable, if the following four guiding principles are followed.

1. Use a private, permissioned blockchain

While the most common vision of blockchain is of a fully public, permissionless network, there are a wide variety of blockchain solutions, many of which are in fact private and require permission to join. The principal point of a public, permissionless network is that any person in any location can become a participant in that blockchain, without registration or restriction, simply by installing the relevant software and downloading a full copy of the blockchain.

Right to erasure	Also known as 'the right to be forgotten', the GDPR introduces a right for individuals to have personal data erased, although this is limited to certain circumstances (Article 17)
Right to rectification	Individuals have a right to have inaccurate personal data rectified, or completed if it is incomplete (Article 16)

Generally, all participants on a public permissionless blockchain can see all the data on the blockchain ledger. Because anyone can join a public permissionless blockchain, it is impossible to ensure participants agree to necessary rules around the protection of personal data.

By contrast, to join, view data on or interact with a private permissioned blockchain network, participants must first obtain authorisation. Private permissioned blockchain networks employ various processes to approve new participants and part of this process can be to ensure all new participants subscribe to a set of rules or terms and conditions that govern their use of the network.

For these reasons, compliance with the GDPR requires use of a private permissioned blockchain.

2. Avoid, if possible, the storing of personal data on the blockchain

The most obvious way to avoid GDPR compliance issues is, predictably, to employ a blockchain solution that avoids processing any personal data. Indeed, one crucial aspect of distributed ledger technology, that data should be replicated and maintained by various participants rather than stored centrally, is somewhat at odds with the GDPR's principles of data minimisation, storage limitation, and purpose limitation. The ideal means to resolve this dilemma is to avoid it altogether.

While keeping a blockchain completely free of personal data will be very difficult to achieve, this should not prevent efforts being made to keep personal data off-chain (as far as it is possible to do so). This may be done, for example, by storing an encrypted anonymous hash of the personal data on-chain, with the underlying and identifiable personal data being kept off-chain and minimising free form data.

However, given the expanded definition of personal data under the GDPR, it is also important to consider the data environment within which the personal information sits, rather than only focusing on information that is clearly, on its face, personal data. After all, personal data under the GDPR also includes information relating to an indirectly identifiable individual, and this means that information which on its own may not be personal data can quickly become personal data when brought together with other information to build a profile of an identifiable individual. Finally, while a blockchain solution may be designed to avoid storing personal data, there are numerous instances where personal data may nevertheless be added to the ledger.

However, blockchain middleware applications (software that sits on top of one or more underlying blockchain networks and facilitates the application of those blockchain networks to particular use cases) could be used to prevent personal data being added to the network by avoiding the inclusion of specific data fields for personal data such as fields for names, phone numbers or email addresses.

These applications could also employ more advanced techniques to recognise and remove personal data from information submitted to the blockchain network. AI or machine learning-based tools can, for example, be employed to recognise and blur faces in images (or anonymise other personal data) before it is submitted to the network.

3. Implement a detailed governance framework

A GDPR-compliant commercial blockchain solution will require a detailed governance framework that is contractually binding on all participants and clearly sets out each party's rights and responsibilities. This is because of:

- the need to ensure that personal data is adequately protected;
- the requirements under the GDPR to establish contractual relationships governing the processing of personal data between parties;
- the legal obligations on data controllers to provide individuals with privacy notices and a means to uphold their personal data rights; and
- the use of established contractual mechanisms to enable the export of personal data across international borders.

The contractual governance framework can be built in such a manner that the GDPR responsibilities of network participants around the provisions of privacy notices, the upholding of data subjects' rights, the response to subject access requests, the restriction of international transfers, and the proper administration of relationships between controllers and processors can all be appropriately addressed.

4. Employ innovative solutions to data protection problems

As discussed above, the immutable nature of blockchain data is the one element of the technology which clashes most obviously with the GDPR, especially the right to erasure and the right to rectification. However, through reliance on innovative solutions such as the use of advanced irreversible encryption (as a means of deletion), or the use of supplementary corrective statements (as a means of rectifying inaccuracies)

there are solutions that enable compliance with the spirit and the policy of data protection legislation, if not yet fully the word.

For example, in relation to the right to erasure, while it is technologically difficult (and expensive) to delete historical blocks of data on a blockchain ("pruning") or delete and rebuild a blockchain ("forking"), it may be possible to delete personal data stored on the blockchain by irreversibly encrypting the data. Under this approach, the encrypted data would remain permanently on the blockchain, but the personal data it contains would be "deleted" from the blockchain by deleting all keys that enable decryption of that data. This is arguably a natural extension of the view held by the German Blockchain Federation (Blockchain Bundesverband)[1] and the UK Anonymisation Network[2] that data is no longer personal data if it has been irreversibly anonymised.

However, the Article 29 Data Protection Working Party (now the European Data Protection Board) previously classified encryption and hashing as pseudonymisation, not anonymisation, though the guidance has not been endorsed by the EDPB[3]. One pseudonymisation technique mentioned by the Working Party included producing a cryptographic hash and then deleting the key to unlock that hash. The opinion did note that employing this technique would make it "computationally hard for an attacker to decrypt or replay the function, as it would imply testing every possible key, given that the key is not available", but it remains unclear whether personal data that is irreversibly encrypted and keyless can be considered to be anonymised for the purposes of the GDPR (and thus theoretically deleted from a blockchain network).

It is for this reason that it is of utmost importance for the European Data Protection Board and national data protection authorities to produce up-to-date, pragmatic and innovative guidance on the interplay between blockchain and the GDPR, especially in relation to innovative solutions to deletion and rectification.

Regulatory guidance required

It is clear that not all of the blockchain challenges posed by the GDPR and other privacy regimes can currently be completely bridged. However, the gap left by those challenges is in fact relatively small, and the fundamental freedoms forming the policy behind such privacy laws can be maintained and protected in particular blockchain environments with the help of an active and pragmatic approach by lawmakers and regulators alike.

Greater engagement by, and co-operation between, regulators, law-makers and blockchain technology developers is now a necessity. The current legal and regulatory obstacles could then be overcome in a manner that facilitates the continued growth and exploitation of blockchain as a technology of great potential.

There is a risk that, if steps are not taken by regulators and lawmakers to bridge the gap between data protection law and blockchain technology, there will be a slowing in (or even end to) advancements in blockchain solutions. Such an outcome would ultimately be detrimental to technological developments having the capacity to deliver substantial benefits to the world as a whole.

[1] German Blockchain Federation (*Blockchain Bundesverband*) "Blockchain, data protection and the GDPR", available here

[2] UK Anonymisation Network "The Anonymisation Decision-Making Framework, 2016", available here

[3] Article 29 Data Protection Working Party, opinion 05/2014 on Anonymisation Techniques (adopted on 10 April 2014), available here

This article was written by Rob Sumroy, Duncan Mykura and Ian Ranson. Slaughter and May advises on all aspects of data protection and privacy. Please contact us if you would like any further information.

Further publications are available on our website.

Rob Sumroy
T +44 (0)20 7090 4032
E rob.sumroy@slaughterandmay.com

Duncan Mykura
T +44 (0)20 7090 3474
E duncan.mykura@slaughterandmay.com

Ian Ranson
T +44 (0)20 7090 3932
E ian.ranson@slaughterandmay.com