Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

GDPR Compliance Questions For Blockchain Firms

By **Daniel Cooper, Charlotte Hill, Sophie Bertin and Gemma Nash**
(October 10, 2018, 2:48 PM EDT)


Daniel Cooper


Charlotte Hill


Sophie Bertin


Gemma Nash

Blockchain technology (a form of distributed ledger technology) is considered as being able to fundamentally change all aspects of today's business. While the technology's claim to fame is its role as the architecture of the cryptocurrency bitcoin, it will certainly play a revolutionary role much more broadly. It is expected that all industries will be affected. When looking at the financial services industry, there are expectations that all parts of it will be impacted: for instance cash payments, trading, clearing and settlement, as well as all middle- and back-office functions. The recent example of Austria emitting government bonds on blockchain gives a glimpse of the potential for change. However, the benefits of blockchain are still to be demonstrated, and some challenges have already emerged. One of them is how the technology can comply with new privacy legislation. In particular, the recently introduced General Data Protection Regulation can be seen as a possible roadblock in terms of the technology's future development.

What is Blockchain Technology?

Put simply, blockchain is a shared immutable digital ledger that records information. The information is stored in blocks which are then added to a chain of other blocks on a decentralized network. Blockchain technology operates through a peer network, where transactions must be verified by participants before they can be added to the chain. However, once they are added to the chain, they cannot be deleted, altered or moved. Each such action will then be recorded as a separate new action. The network can either be public, which is so far the most common occurrence of blockchain, in that everyone can access the network, or it can be private, as in closed to a certain set of individuals (or institutions) who have to be authorized to access the network. It can also either be permissioned, so an individual or institution needs authorization to be able to access and add to the network, or they can be permissionless, as in anyone can post to the network.

These varying features of a blockchain network raise various GDPR compliance questions. For instance, one can ask how can the immutable ledger comply with data subject rights of deletion and rectification, and how does a decentralized network fit within the framework of the GDPR?

Compliance with Data Subject Rights

The GDPR applies to personal data which is defined as "any information relating to an identified or identifiable natural person", and as such the GDPR will apply to a blockchain network where personal data (e.g., a person's name or address) is directly stored on the blocks within the chain.

Where blockchain stores and processes personal data it will have to comply with data subject rights such as the right to rectification, where personal data concerning them is inaccurate, and also the right for their data to be deleted. Personal data which is directly stored in a block will not be capable of being rectified or deleted, as the ledger is immutable in order to ensure the security and accuracy of the information stored on it. While the right to deletion is subject to conditions, when it applies, regulators expect that all relevant data is permanently deleted from the relevant records or anonymized. In an immutable ledger, this may be a challenge, as all changes leave a trace in the chain. A similar issue arises from the record keeping obligations, where data shall only be stored for as long as necessary. Such retention times can be defined by law or specified e.g. for regulatory reporting purposes. At the end of the retention time, the data shall be deleted. This, again, might prove a challenge for blockchain.

Ensuring Compliance in a Decentralized Network

In a decentralized network questions arise on who within this network falls into the roles of "data controllers" and "data processors" as envisaged under the GDPR, and therefore who is responsible for the obligations and responsibilities that come with these roles. In a private blockchain this may be easier to reconcile where the technology is being used solely by one company as part of its back-office functions. However, where the network is public, meaning anyone can post and access the ledger, who is the ultimate owner may be far less clear. In theory, anyone who accesses and posts to the network may be considered a (joint) data controller and bear the responsibilities associated with it.

The cross-border nature of many blockchain networks can also prove a challenge, as under the GDPR, the data subject can ask to know where the data is located. Given that (full) nodes have in theory a copy of the whole chain and that those nodes can be located anywhere in the world, complying with this requirement can indeed prove to be a challenge.

Next Steps

Various regulators have already started to pay attention to these potential challenges. For example, the U.K. Financial Conduct Authority recently published a feedback statement, in response to its discussion paper on distributed ledger technology, in which it commented on the challenge that blockchain technology faces with complying with the GDPR when processing and storing client data. However, while the FCA acknowledged that there are "significant challenges," it believes that the combination of the GDPR and the use of DLT has the potential to improve the way in which firms collect, store and process private information, which it believes would result in "significantly improved consumer outcomes."

The European Commission also recently launched the EU Blockchain Observatory and Forum which ran a series of workshops on the impact of the GDPR on blockchain technology.

Given the number of open questions, the use of blockchain technology will need careful consideration to ensure compliance with GDPR. This compliance is best ensured prior to launching the blockchain. In addition, in some cases, further guidance from regulators may be necessary.

Daniel P. Cooper and Charlotte Hill are partners, Sophie Bertin is a senior adviser and Gemma Nash is an associate at Covington & Burling LLP.