Blockchain and data protection: the main concerns

DENTONS

February 25, 2019

As one of the most important drivers of the digital industrial revolution, blockchain technology and its applications are today one of the most discussed global topics. A blockchain can be defined as a decentralised database that keeps track of an unlimited number of data assets and transactions through a peer-to-peer network. It is a registry maintained by a consensus algorithm and stored in a network of "nodes", *i.e*. computers that allow (also personal!) data to be included in "blocks" that are chained (hashed) one to another.

Blockchain's usage is no longer limited to digital crypto currencies, as blockchain databases may be deployed in innumerable circumstances and scenarios, including, for instance, within the financial services and insurance sectors for money transfer, peer-to-peer lending and transfer of securities, as well as automatic execution of contracts.

The advantages of blockchain include, amongst others, transparent and tamper-proof processes, disintermediation and cost reductions, security (because of the hashing process), and more generally an additional layer of trust due to the fact that each transaction is verified by a wider audience of "nodes".

Regulators are setting up a legal framework for operating a blockchain in a (legally) safe environment, including blockchain-based smart contracts. In this respect, Italy is one of the first jurisdictions that has passed specific legislation on blockchain (which will be discussed in the next issue of our TMT Bites).

That said, the relationship between blockchain and other distributed ledger technologies (DLTs) to personal data protection, including the provisions of the General Data Protection Regulation no. 679/2016 (the "GDPR"), has yet to be fully addressed.

In essence, albeit "technology neutral", the GDPR is based upon a "centralised" approach, with a data controller possessing full and ultimate responsibility over data processing and storage, with any data processor under the controller's full control. But blockchain is a form of distributed ledger, and by definition "decentralised".

This implies, particularly with public and unpermissioned blockchains, a difficulty in identifying the data controllers, *i.e.* the entity determining the means and purposes of data processing. In fact, in the absence of a centralised determination of such means and purposes, either no node is a data controller, or, more likely, each node is a data controller as it is not subject to external instructions.

Such nodes may be located in various jurisdictions, there being no physical limits (or control) applied. This also implies potential data transfers to jurisdictions that do not grant an adequate level of protection of personal data.

In addition to the practical difficulties in effectively identifying the nodes to which to submit the data request, certain rights may not be effectively exercised by the data subject. For instance, the GDPR also provides for the principle of data minimization, whereby, among other things, data have to be processed for the specified and explicit purposes and for the time strictly necessary for the processing. In most instances, however, the data, once added to the blockchain, will remain stored in perpetuity, as part of an append-only database.

Similar issues arise for the right of amendment and rectification, as well as the right to be forgotten, as it is generally impossible to erase the data (apart from some exceptional cases). This issue may only partially be addressed by adding data that rectify the previous data.

As is happening with artificial intelligence, regulators are facing the challenge of protecting the fundamental rights of the individual, whilst not affecting the technology and innovation. This is a key challenge as, where appropriately managed, the GDPR principles of data protection by default and by design will be key in ensuring that blockchain will in fact allow more and data sharing. This may imply, for instance, additional layers of cryptography or the combination of blockchain and off-chain storage.

The regulatory authorities will no doubt take further steps, on a European and national level, to tackle these concerns. In the meantime, when using blockchain-based technologies and databases, a careful assessment through a data protection impact assessment remains advisable.

Let us know if you require further information, and don't forget to sign up for our TMT Bites!

Your Key Contacts

Giangiacomo Olivi
Partner, Europe Co-Head of
Intellectual Property, Data
and Technology, Milan
D +39 02 726 268 00
M +39 344 27 62 550
giangiacomo.olivi@dentons.com