THE
NATIONAL LAW REVIEW

The CNIL Publishes Report On Blockchain and the GDPR

Article By Gemma Nash
Daniel P. CooperSophie Bertin
Covington & Burling LLPInside Privacy

Communications, Media & Internet
Global
European Union
France

Wednesday, November 14, 2018

On November 6, 2018, the French data protection authority (the “CNIL”) published a report that discusses some of the questions raised by the use of blockchain technology and perceived tensions between it and foundational principles found in the General Data Protection Regulation (the “GDPR”). As we noted in an earlier blog post on this topic, some pundits have claimed that certain features of blockchain technology, such as its reliance upon a de-centralised network and an immutable ledger, pose GDPR compliance challenges. The CNIL has attempted to address some of these concerns, at least in a tentative manner, and further guidance from EU privacy regulators can be expected in due course.

De-centralised network

The CNIL acknowledges that EU data protection principles have been designed “*in a world in which data management is centralised,*” and where there is a clear controller of the data (“data controller”) and defined third parties who merely process the data (“data processors”). Applying these concepts to a de-centralised network such as blockchain, where there are a multitude of actors, leads to a “*more complex definition of their role.*” In brief, EU data privacy rules are the square peg to blockchain’s round hole.

Notwithstanding this, the CNIL considers that participants on a blockchain network, who have the ability to write on the chain and send data to be validated on the network, must be considered data controllers. This is the case, for instance, where the participant is registering personal data on the blockchain and it is related to a professional or commercial activity. By contrast, according to the CNIL, the miners, who validate the transactions on the blockchain network, can in certain cases be acting as data processors. As a consequence, data processing agreements would need to be in place between the data controllers and the data processors on any blockchain network.

The CNIL further considers that where there are multiple participants who decide to carry out processing activities via a blockchain network, they will most likely be considered “joint controllers,” unless they identify and designate their roles and responsibilities in advance.   Individuals who use the blockchain for personal use (i.e., individuals who access the network to buy and sell a virtual currency), however, would not be data controllers as they can rely on the “*purely personal or household activity*” exception.

Immutable ledger

As identified in our previous blog post on this topic, one of the most widely recognised tensions between blockchain and the GDPR is the inability to delete data on the network. The CNIL gives great weight to this concern in its report, particularly in relation to ensuring compliance with data privacy principles such as data minimisation, but also for ensuring the effective exercise of a data subject’s rights. For example, due to the inability to delete data on the network, the CNIL considers that a data subject’s right to erasure is “*technically impossible to grant…when data is registered on a blockchain.*” The CNIL can offer no real solution to this problem.

More positively, the CNIL seems less concerned with personal data such as public keys, which allow participants to be identified on the network (known as participant identifiers), as these are “*essential to the blockchain’s* *proper functioning*" and therefore cannot be further minimised. Consequently, their retention periods will be in line with the duration of the blockchain's existence. However, any additional personal data stored on a blockchain network is likely to cause much greater concern from a privacy compliance perspective.

CNIL Recommendations

For companies wishing to use blockchain technology, the CNIL makes the following recommendations:

- Companies should carefully assess whether the use of blockchain technology is really necessary, particularly the use of a public blockchain. While hardly a ringing endorsement of blockchain, the CNIL at least do not flatly challenge its deployment.
- Where groups of companies wish to carry out processing operations based on a common purpose on a blockchain, they should clearly define and allocate the data controller responsibilities among the members of the group.
- Whenever possible, personal data (i.e., excluding participant identifiers) should be processed outside of the blockchain (particularly where the data is in cleartext), or a cryptographic solution which makes the data practically inaccessible should be used, such as (i) "commitments" (which in effect allows data to be frozen), (ii) a hash generated by a keyed hash function on the data, or (iii) a ciphertext of the data.
- To ensure effective security for permissioned blockchains, companies should evaluate the minimum number of miners that could lead to collusion and as such overpower the chain, and ensure that the number of miners are always above this minimum.
- Companies should also establish technical and organisational procedures that reduce the potential for "algorithm failure" (i.e., vulnerabilities in the system), which should include an emergency plan in the event of such a failure.

Unanswered questions

Frustratingly for industry, the CNIL report leaves as many questions unanswered as it addresses, such as:

- **How to manage data processors on a public blockchain**. After observing that certain participants on the blockchain, such as miners who validate transactions, may be processors, the CNIL concedes that applying data processing contracts that comply with Article 28 of the GDPR may be aspirational. While on private and permissioned-based blockchains entering into such agreements is more straightforward, on a public blockchain there are practical difficulties with formalising these relationships. The CNIL is carrying out a further in-depth assessment of this particular concern.
- **Transfers outside the EU on a public blockchain**. Where participants on a blockchain network are spread across numerous countries, including outside the EEA, compliance with data transfer obligations will need to be addressed. The CNIL recognises that for permissioned blockchains, safeguards such as binding corporate rules and/or standard contractual clauses will be easier to implement. For public blockchains, appropriate cross-border safeguards will be harder to implement.
- **Data erasure.** While the CNIL recognises that there are some methods for limiting the durability of data on the blockchain, it still questions the extent to which these solutions ensure full compliance with the GDPR, particularly as the solutions do not "*strictly speaking, result in an erasure of the data.*"

For these more complex concerns, in particular the issue of data erasure, the CNIL states that "reflection at the European level is *essential*" (emphasis added). The CNIL intends to work with other European data protection regulators to establish "*a strong and harmonised approach*," as well as contact other national regulators (such as financial regulators) to establish "*a foundation for inter-regulation.*"

© 2019 Covington & Burling LLP

Source URL: https://www.natlawreview.com/article/cnil-publishes-report-blockchain-and-gdpr