Updates
October 12, 2018

French Data Protection Authority Issues Guidance on Application of Blockchain to the GDPR

On September 24, 2018, the French data protection authority, Commission Nationale de l'Informatique et des Libertés (CNIL), became the first data protection authority to issue written guidance on the intersection of the use of blockchain technology and the General Data Protection Regulation (GDPR). Due to the decentralized and permanent nature of the blockchain, there is an inherent tension between blockchain technology and the GDPR, particularly with respect to data subject rights and data storage limitation principles. Therefore, the CNIL guidance provides some welcome clarification on how it views these inherent tensions, although the CNIL left open certain important issues that will require deeper analysis and explanation in the future. The summary below was prepared based upon an unofficial translation of the CNIL guidance, and therefore may change if and when the CNIL releases an official English translation of the guidance. Our high-level takeaways based on the CNIL guidance are as follows:

- The legal analysis of whether the GDPR applies to a blockchain must be conducted on a participant-by-participant basis. Some participants on a blockchain may be subject to the GDPR while others may not.
- The greater the ability of a participant to intervene and influence blockchain transactions, the more likely such a participant is subject to the GDPR.
- Whether a participant is a controller or a processor, as such terms are defined under the GDPR, is a determination based on the particular facts and circumstances, influenced by the architecture of the blockchain and the types of users who engage with it.
- Data minimization principles apply to some but not all aspects of blockchain technology. Notably, there is no data minimization requirement for public addresses and public keys.

The following constitutes a brief summary of the CNIL guidance broken into categories based upon the most important questions the CNIL addressed:

Generally, who is subject to the GDPR when using a blockchain?

The CNIL is of the opinion that participants engaging with blockchain networks are responsible for the treatment of personal data under two general circumstances: when (1) the participant is a natural person and the processing of data is related to a professional or commercial activity (i.e., not exclusively a personal or household activity, which is exempt under Article 2 of the GDPR); and (2) the participant is a legal entity that enters personal data on a blockchain.

For a natural person, the CNIL gives the example of a notary entering property title information on a blockchain on behalf of a client. For a legal entity, the CNIL gives the example of a financial institution entering personal data of its customers onto a blockchain as part of its customer management processes.

Are miners data processors?

An important insight from the guidance relates to the CNIL's treatment of public blockchain miners (i.e., the individuals and entities that compete to process and verify transactions on blockchain networks in exchange for network fees). According to the CNIL, there are circumstances where miners would not be responsible for the processing of personal data and therefore would not be subject to the GDPR, so long as their activities are

limited to validating transactions submitted to them by other parties and they do not intervene in the transaction flow or determine the purpose or means of processing. One possible interpretation of this position is that where processors who did not design or control the way the protocol works, but are instead simply validating and verifying blocks according to the protocol, and where they are not participating in the transactions themselves in any way, they are not considered "processors" of the data within those transactions.

Although this guidance provides some clarity on how one important regulator views miners under the GDPR, questions are likely to persist regarding what types of activities may constitute sufficient intervention that results in a miner being deemed a processor. For example, would it be considered processing for a miner to prioritize certain transactions over others or for a miner to refuse to process transactions submitted from blacklisted addresses? These nuances are not dealt with specifically in the guidance.

Elsewhere in the guidance, the CNIL does provide additional color as to mining activities that *would* constitute processing on behalf of controllers. It provides an example of a group of insurance companies utilizing a permissioned blockchain solution that requires the insurance companies to mine blockchain transactions on behalf of customers. In such a permissioned system, the CNIL states that the group may designate one insurance company as a controller (most likely the entity entering the customer's personal data on the blockchain) and the other insurance companies would be designated as processors. However, it remains unclear whether this interpretation of processing would still apply outside the context of permissioned blockchain systems, where there may not be a clear controller. The CNIL states that it is still considering the issues raised by miners in the public blockchain space. Presumably, there will be more guidance provided on this point in the future.

What happens if several organizations decide to jointly implement a blockchain solution?

The CNIL recommends that groups with a common purpose of implementing blockchain processing solutions create legal entities (e.g., associations, joint ventures) to manage controller responsibilities under the GDPR. Similar to the broad application of the GDPR to associations and consortiums, participants in an association should identify a participant that makes decisions for the group and designate it as the controller. As with other associations, if a blockchain association cannot designate one of the participants as the controller, all of the participants have potential controller responsibility.

How are smart contracts and their developers treated under the GDPR?

According to the CNIL, smart contract developers may be viewed as processors under the GDPR depending on their activities, even if the processing is accomplished via smart contract (i.e., a computerized transaction protocol that executes the terms of a contract[1]). The CNIL gives the example of a software developer who develops a smart contract for an insurance company that automates the compensation of passengers for flight delays. The guidance states that the developer in this example would be a processor for the insurance company, which would in turn be the controller. While that might make sense in the context of a developer who is involved in the ongoing functionality of the smart contract, it is less clear from the guidance what status a developer would have if the smart contract operates without the technical ability or legal right/obligation of the developer to intervene after the smart contract is deployed and is truly automated. Arguably, such a developer would be a mere provider of the technology that enables the processing of personal data but not himself a controller or processor of such personal data.

Elsewhere in the guidance on smart contracts, the CNIL emphasizes that data subjects should be able to intervene and challenge a decision after a smart contract has been executed. The CNIL goes further to state that it would be appropriate for the controller to provide for the possibility of human intervention regardless of what is registered on the blockchain. This position runs counter to many of the benefits offered by blockchain technology and does not seem to give appropriate credit to the fact that smart contracts are intentionally designed to function without human intervention. One of the virtues of smart contracts is the elimination of potential and

unwanted human intervention altogether. Requiring access, either by developers or others, creates vulnerabilities for smart contracts that may eliminate or stunt their ability to act securely or as trusted and impartial intermediaries.

What about the right to erasure?

The CNIL does not elaborate on the conceptual difficulties related to requests for erasure by data subjects (Article 17 of the GDPR) when personal data is entered on or accessible through a blockchain. However, it does provide some guidance on technical workarounds, particularly when data is referenced on a blockchain (e.g., via a hash value) and is stored elsewhere (i.e., "off-chain" or not on a blockchain). In essence, if the data stored on a blockchain is only referencing data stored off-chain, controllers may comply with requests for erasure from data subjects by removing the underlying data. Similarly, if the underlying data can only be accessed or verified via a specific private key, then making the private key inaccessible may also constitute an effect similar to the erasure of data. Ultimately, the CNIL punts on further analysis, stating that a more thorough evaluation of these possible solutions is needed. This particular privacy principle deserves significant study as it pertains to the immutable nature of most blockchains. It may be that regulators and technologists need to rethink how to balance data integrity (which blockchain immutability can enhance) with a right to erasure. We also need to consider the practicality of honoring a data subject's right to erasure given the fact that in many instances there is no central authority responsible for honoring or executing the rights of individual participants. Certainly, more discussion and guidance is required to provide certainty regarding how blockchain participants can avoid running afoul of this and other principles.

How to minimize risk when data processing relies on blockchain technology?

The CNIL provides some guidance on how individuals and companies might minimize their GDPR risk around blockchain technology. First, the CNIL recommends that companies seeking to process large amounts of personal data using blockchain technology rely on private blockchains over public blockchains. The CNIL favors private blockchains largely because of the geographic issues associated with public blockchain node operation. Most public blockchain nodes can be located anywhere in the world and can be operated by any natural person or entity that has a computer that maintains a copy of the blockchain ledger. This presents problems under the GDPR, which restricts the transfer of personal data to countries that do not ensure an "adequate" level of protection without the appropriate legal safeguards in place. Note that the United States is considered a country that does not ensure an "adequate" level of protection under the GDPR. The CNIL argues that permissioned blockchains can allow for tighter control over the jurisdictions in which nodes are operated, thus better complying with the geographic limitations imposed by the GDPR. This guidance may run counter to the objectives of public blockchain networks. Public blockchains often intend to be borderless: the same protocol and the same ledger exists across all participants in all jurisdictions.

A second CNIL recommendation relates to how data is stored using a blockchain. The CNIL notes that there is tension between the principle of data retention periods (Article 5 of the GDPR) and the permanence of blockchain transaction information. Without reaching a conclusion as to whether or not this trait makes it impossible for a blockchain to comply with the GDPR, the CNIL offers some guidance on data minimization techniques. For public address hash values and public keys there is no data minimization option available due to the technical specifications of blockchains. For payload data committed to a blockchain, data minimization principles should be applied such that the data is cryptographically secured via encryption or by including references to the underlying data (stored elsewhere) in the form of a hash value in the payload.

The CNIL also recommends that all blockchains establish technical and organizational procedures, including an emergency plan that allows the underlying algorithms to be modified when a vulnerability is identified. Finally, the CNIL encourages blockchain participants to document all changes to the software used to create transactions

to ensure that the planned permissions are in line with actual implementation.

What remains unclear?

In short, there are many GDPR topics that the CNIL did not cover in the guidance. For example, the CNIL recognizes that the structure of the blockchain necessitates that certain identifiable information cannot be removed or further minimized, such as public keys. However, one pressing open question is whether personal data that is cryptographically secured, including through hashing or use of a cipher, can ever be considered sufficiently anonymized to fall outside the scope of the GDPR.

Other pressing issues that remain unclear include the following:

- Is the imposition of geographic limitations on the transmittal of information outside the European Union even possible on public blockchain networks, and if not, how will the regulators respond?
- Can a deployed and unchangeable smart contract be GDPR-compliant?
- Are there limits to the applicability of the data retention period for blockchain transaction information?

Steps to Take Now?

It is clear that privacy protocols/legislation are becoming more protective; increasingly implicating large swaths of technology. It may be faster and cheaper for companies who are developing blockchain technologies to build them in a manner that is at least substantially compliant with the GDPR and other similar laws that are taking effect around the globe. It is also clear that the regulators, legislators, technologists, developers, and members of the public should continue to debate and study these problems to seek a balanced approach that protects privacy without impinging technology that, in its final form, may end up protecting privacy and data security effectively.

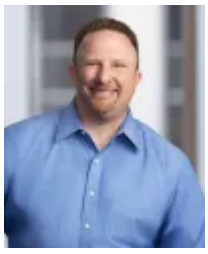
Overall, the CNIL guidance is a strong first step in helping participants understand how regulators view these challenging issues. The CNIL commendably took the proactive approach of embracing GDPR-compliant blockchain technologies and we look forward to additional guidance in the future.

Should you have any questions regarding these developments and how they might apply to you or your business, please contact counsel.

ENDNOTES

[1] The term "smart contracts" was coined in 1994 by Nick Szabo in his article titled, "Smart Contracts," available at http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vw

Authors



Joseph P. Cutler

Partner
JCutler@perkinscoie.com 206.359.6104

Explore more in

Privacy & Security Blockchain, Digital Assets & Custody

Related insights

Update

CFPB Finalizes Proposed Open Banking Rule on Personal Financial Data Rights

Update

FDA Food Import and Export Updates for Industry