Proskauer

Is Blockchain Technology Compatible with GDPR? French Data Protection Regulator Provides Guidance

Blockchain and the Law Blog on **November 28, 2018**

Uncertainty regarding the compatibility of blockchain technology and the European Union's General Data Protection Regulation (GDPR) has often been highlighted as a potential obstacle to the development and widespread implementation of blockchain systems involving personal data.

To address tensions between blockchain technology and the GDPR, Commission Nationale de l'Informatique et des Libertés (CNIL), the French data protection regulator, published an initial report analyzing certain fundamental questions regarding the interaction between blockchain technology and the GDPR's requirements (the "Report"). The Report was the first guidance issued by a European data protection regulator on this topic.

CNIL's Approach to Identifying Blockchain Data Controllers and Data Processors

The Report highlights the challenges of identifying data controllers and data processors in the blockchain context – an important distinction that determines which set of regulatory obligations applies.

In discussing the likely classification of the various types of persons and entities involved in a blockchain, the CNIL primarily distinguished between (i) participants (i.e., those who transact on the blockchain) that have the ability to determine what data will be entered into a blockchain or have permission to write on it or cause data to be written to it, and (ii) miners or other validators (i.e., those who do not transact and instead validate transactions submitted by participants). The CNIL also provided an analysis as to how to classify smart contract developers and natural persons who enter personal data in a blockchain, distinguishing, with respect to the latter, between those engaging in personal or household activities and those engaging in professional or commercial activities.

- **Participants:** According to the CNIL, because the participants on a blockchain determine the purposes and means of processing of the personal data (e.g., data formatting, use of blockchain technology for such processing, etc.), they should be deemed data controllers. If a group of participants establishes a blockchain for a common purpose, the CNIL recommends designating a data controller by either creating a company for the purpose of being the controller or contractually designating one of the participants as the controller (in which case the other participants may be considered processors). In the absence of such an arrangement, all participants could be deemed joint controllers under the GDPR.
- **Miners/Validators:** Since validators only validate data to be recorded on a blockchain, the CNIL believes that they are likely not data controllers. Validators can, however, be deemed data processors if they process personal data on behalf of a controller – for example, by executing the instructions of the controller when they verify a transaction submitted by the controller. Article 28 of the GDPR imposes an obligation in such a case to have a written contract in place, which the CNIL acknowledged as potentially posing a number of practical issues, especially in blockchain networks in which participants and validators do not have formal agreements with each other.
- **Natural persons who enter personal data in a blockchain for personal and household activities, as opposed to as part of professional or commercial activities:** In the CNIL's view, a natural person who sells or purchases cryptocurrency, for example, for his or her own account is not a data controller, whereas a natural person that conducts such transactions as part of professional or commercial activities (e.g., on behalf of other natural persons) may be considered a data controller.
- **Smart contract developers:** The CNIL explains that smart contract developers could, depending on the circumstances, be considered either controllers or processors (or neither), as is the case for other types of software developers. For example, a developer that processes data on behalf of the blockchain participant could be considered a processor, whereas a developer that participates in determining the purposes and means of processing could be considered a controller. The point at which a smart contract developer falls into either (or neither) of those categories is not yet clear.

Permissioned and Public Blockchains

In the Report, the CNIL recognizes that the GDPR was designed to respond to a world of centralized data management, whereas a key feature of blockchain technology is its decentralized model. The CNIL notes that public blockchains pose a greater challenge for GDPR compliance than permissioned (also referred to as "private") blockchains. With respect to public blockchains, the CNIL encourages the development of solutions that would facilitate putting requisite contractual agreements in place between the participants and validators if the validators meet the criteria to be considered as data processors.

Minimizing Data Protection Risks in the Context of Blockchain Technology

- **Privacy by design:** Article 25 of the GDPR requires data controllers to establish appropriate technical and organizational measures to implement data protection principles and safeguard individual rights (a concept often referred to as "privacy by design"). In the CNIL's view, given the GDPR's requirement of privacy by design, blockchain technology may not be a suitable technology where a transfer of personal data outside of the EU is involved. With respect to public blockchains, the data transfer mechanisms commonly used to enable such data transfers to comply with the GDPR (model contracts and binding corporate rules) may be difficult to implement because controllers may not be able to exercise control over the validators' locations or effectively enter into the necessary written agreements with them all. Where a transfer of personal data outside the EU is involved, permissioned blockchains are preferable to public blockchains because the controller can exercise more control over how personal data is treated, and the commonly used data transfer mechanisms are more compatible with permissioned blockchains, in which participants are approved, known and more likely to have formal business relationships outside of the blockchain.
- **Limited Retention Periods:** Under the GDPR, personal data cannot be kept indefinitely. A retention period must be determined based on the purpose for which the data is being processed. The CNIL holds the view that the limited retention period required under the GDPR is, on its face, a clear incompatibility between the typical blockchain structure and the GDPR. It notes as an example that certain data must be kept for the lifetime of a typical blockchain – namely, the participants' identifiers or public keys – since the architecture of a blockchain usually requires identifiers to remain in the blockchain.
- **Encryption:** The CNIL generally advised that unencrypted personal data should be stored off-chain and that any personal data stored on a blockchain should be registered in the form of (i) a cryptographic mechanism known as a "commitment" (which allows one to "freeze" data in such a way that it is both possible – with

additional information – to prove what has been frozen and impossible to find or recognize such data by using the sole "commit"), (ii) a hash generated using a hash function with a key, or (iii) an encryption ensuring a high level of confidentiality. The CNIL did acknowledge that there may be some circumstances in which personal data that is subject to lesser cryptographic protection (or even personal data that is unencrypted) may be stored on a blockchain in compliance with the GDPR. It noted, however, that this would only be acceptable where the purpose of processing warrants such storage (perhaps for data controllers that have a legal obligation to make certain information public and accessible, the CNIL suggested) and a data impact assessment shows that the associated risks are minimal for the applicable data subjects.

Data Subject Rights Under the GDPR

The CNIL acknowledged that certain data subject rights under the GDPR (the right to be informed, the right of access and the right to data portability) can be satisfied in the context of blockchain technology. However, it noted that other data subject rights under the GDPR, including the right to object, the right to rectification and the right of erasure, conflict with fundamental attributes of a classic blockchain. With respect to those rights, the CNIL suggested that, although an imperfect solution, implementing technical measures to achieve results that are practically the same as those intended by such rights may be a path to deemed compliance with those rights. For example:

- Regarding the right of erasure, the CNIL stated that using technical solutions that render the data "almost inaccessible" (e.g., by removing the private key from the hash function, which would make verifying which information was hashed in the first place impossible) could be one way to achieve compliance, even though the data technically still resides on the blockchain.
- Regarding the right to rectification, the CNIL noted that the rectified data could be entered into a new block in a subsequent transaction that would supersede the previous one. The superseded transaction would remain in the blockchain, however, and to address this issue the CNIL suggested that the data containing the error could then be treated with the same technical solutions as the ones recommended by the CNIL to render data "almost inaccessible" in the context of the right of erasure.

Automated Decision-Making and Smart Contracts

The CNIL also analyzed the interaction between blockchain technology and the data subject's right not to be subject to a decision based solely on automated processing that produces legal effects concerning him or her or similarly significantly affects him or her (referred to as "automated individual decision-making").

The GDPR provides that automated individual decision-making is only permitted in limited instances, including when the data subject has provided explicit consent or if it is necessary to perform a contract with the data subject. The CNIL acknowledges that, in the case of smart contracts, automated individual decision-making may be necessary for the performance of a contract and therefore may be permitted under the GDPR.

In the context of smart contracts, the CNIL suggested that controllers should provide for the possibility of human intervention to allow automated decisions to be challenged by data subjects, even if the contract has already been executed.

The CNIL recognized that the Report is a preliminary analysis, acknowledged that a number of questions remain unanswered, and invited the blockchain sector and other EU data protection regulators to find creative solutions for reconciling blockchain technology with the strict requirements of the GDPR. The CNIL also expressed an interest in working with other regulators on specific blockchain regulations, such as, for example, with the French financial markets regulator, Autorité des Marchés Financiers (AMF). In October of 2018, the Assemblée Nationale (the French equivalent of the House of Representatives) adopted a proposed regulation regarding crypto assets and initial coin offerings (ICOs) that, if approved by the French Senate, would result in the involvement of the AMF in certain ICO transactions, making it likely that the CNIL and the AMF will collaborate and opine on the specific data privacy issues raised by ICOs.

View Original

Related Professionals

- **Stéphanie Martinier**
  Partner