Read this post online

The blockchain facing GDPR

The blockchain is a technology a personal data processing can rely on. Its very specific characteristics raise difficulties for the implementation of the obligations imposed by the General Data Protection Regulation (GDPR).

On September 24, 2018, the CNIL (The French Data Protection Authority) issued its first analysis and recommendations for those who wish to use the blockchain when they process personal data.

The blockchain constitutes a "*method for recording continuously generated data, in the form of blocks that are linked to each other in chronological order of validation, each block and its sequence being protected against changes*"[1].

It is in particular used for the cryptocurrency for which it is a sort of public register of the transactions, like the bitcoin, which is far from being the only cryptocurrency. The use of the blockchain can rely on so-called "smart contracts" which are computer programs which are self-executing: "if" the program notes that a pre-programmed condition is met, "then" it executes the terms of the contract. The smart contracts may also be used for an ICO (*initial coin offering*), which is a mechanism to fund a project by issuing cryptocurrencies or tokens. The bill on business growth and transformation (known as the "PACTE" Bill in France) currently in debate in France provides for a legal framework for such ICO.

The login, i.e. the keys[2], and the data recorded on the blockchain, if they relate to a natural person who is identified or identifiable, can be considered as personal data.

How to comply with the GDPR's provisions taking into account the uncommon characteristics of the blockchain?

On September 24, 2018, the CNIL issued its first analysis and recommendations for those who wish to use the blockchain when they process personal data[3].

Who is the data controller?

The identification of the data controller – defined as the one who determines the purposes and the means of the data processing – is essential. The obligations provided by the GDPR are on him mostly.

For the CNIL, the blockchain is not per se a data processing, but a technology. All the persons who store or move data are not necessarily data controllers.

Among these persons, the CNIL makes a distinction between the "accessors", who have the right to read and hold a copy of the chain, the "miners" who validate a transaction and create blocks by applying blockchain rules for "acceptance" by the community, and the "participants" who have the right to make entries (i.e., make a transaction for which they request validation) and who determine the purposes (goals to achieve with the data processing) and the means to process (format of the data, use of the blockchain, *etc*.).

According to the CNIL, only a participant can be considered as a data controller:

- When he/she is a natural person and that the data processing is linked to his/her commercial or professional activity;
- When it is a legal entity who decides to register a personal data.

When a group of bodies decides to implement a data processing on a blockchain for a common purpose, the CNIL recommends that the participants take a common decision regarding the responsibility 1) either by creating a legal entity and appointing such entity as the data controller; 2) by designating the participant who will make the decision for the group as the data controller. By default, all participants may be considered as being jointly and severally liable.

Is there a data processor?

In certain cases, some persons may be considered as data processors. One of the big changes brought about by the GDPR consisted precisely in requiring the data processors to comply with certain obligations.

This is the case for the developer who makes a smart contract on behalf of the participant who is the data controller.

The miners can also be considered as data processors since they execute the data controllers' instructions when they check that the transaction complies with the technical criteria.

They shall enter into a contract with the participant who is the data controller, setting forth each party's obligations and referring to Article 28 of the GDPR.

Such an obligation to enter into a contract raises difficulties when the blockchain is public (i.e. open: the protocols of the blockchain are open source for writing and reading without restriction), which the CNIL simply mentions, encouraging the use of innovating solutions.

How to minimize the risks?

Minimization requires first of all to limit the use of the blockchain when it is really necessary. The protection of private life from the beginning, the Privacy by Design, also requires the data controller to think at the very beginning of the adequacy of its choice to use the technology to process the data.

Regarding the data transfers outside the EU, and when the blockchain is with permission, minimization includes using the actual solutions, such as the binding corporate rules or the standard contractual clauses. However, for the public blockchain, the CNIL acknowledges that it is very difficult for the data controller to use such solutions.

The issue of the personal data storage remains the trickiest one since one of the blockchain features is the impossibility to change or delete the data once it is recorded: Once the block to which the transaction has been integrated has been accepted by the majority of participants, the transaction cannot be modified technically.

The CNIL suggests however a few things to “optimize” the personal data storage.

To the extent that the identifiers of the participants, i.e. their public keys, are essentials for the functioning of the blockchain, the CNIL says that it is not possible to minimize risks any further: the duration of their storage shall be the same as the duration of the blockchain.

Regarding the additional data recorded on the blockchain, the CNIL recommends to use the options where the data is processed outside the blockchain or that the data is recorded on the blockchain by order of preference:

- In the form of a cryptographic commitment, or
- in the form of a fingerprint of the data obtained through a keyed hash function, or at a minimum,
- in the form of a cipher.

If none of these options is possible, and when it is justified by the purpose of the data processing and that a privacy impact assessment has shown that residual risks are acceptable, the data can be stored either with an unkeyed hash function, or, in the absence of any other possibilities, unencrypted.

How can people exercise their rights?

For the CNIL, the right to be informed, the right to access or the portability right does not raise any specific difficulties.

If it is not technically possible to delete data, the CNIL notes that the choice of the format used to store the data via a cryptographic process helps to get close to deletion: the deletion of the data stored outside the

blockchain and the information required for the verification allow to cut the accessibility to the proof recorded on the blockchain, by rendering it difficult if not impossible to obtain.

[1] IT and Internet vocabulary (list of adopted terms, expressions and definitions), Official Journal of the French Republicn°0121 of May 23, 2017, text n° 20

[2] The private key enables the user of a blockchain to initiate a transaction by signing his/her message digitally through cryptography while the public key serves as an address on the blockchain (known to anyone, it allows an issuer to designate a receiver).

[3] Available @ https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data