French DPA CNIL on Blockchain

Summary of the Opinion of the French DPA CNIL

Jörn Erbguth, October 1st, 2018

The CNIL published "Premiers éléments d'analyse" on September 24. The original can be found here https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf.[1]
I want to state how I understand the opinion of the CNIL. Remarks in *italics* are my personal opinion.

Controller

The CNIL starts with the statement that participants who are able to write to the blockchain because they can sign transactions and send them to a blockchain can be regarded as controllers. Miners on the other hand are not regarded as controllers.
When I published this idea at end of 2017 in Zeitschrift für Datenschutz ZD 2017, 560, the reviewers asked me to change my views, but I resisted. If miners are not considered controllers then I would not consider node operators controllers either.
This is different if blockchain participants coordinate among one another with a common purpose. In this case, they should either found an organization which takes over the responsibility or they are jointly responsible.

Personal Activity

When a natural person puts personal data on a blockchain and this is part of a personal or household activity, the GDPR does not apply.

Smart Contract Developer

Smart contract developers could be regarded as processors.
This idea is a bit hard to swallow, especially since smart contract developers develop just the smart contract code and have no influence over who uses this software. Once on the blockchain, they often do not have any possibility to modify the software. The smart contract is even open for inspection by anybody so that people can see what they are using.
This idea of the CNIL would only make sense if they regard all developers of customized software as processors. Taking this thought further would mean that independent software developers are controllers. This has a large range of negative consequences for software development in general and to open source software development in particular.
We will see how other DPAs will buy into the idea of extending GDPR responsibilities to software developers in the future. In any case, I do not see that a special treatment for smart contract developers is warranted.

---

[1] *The CNIL is not the first DPA to publish a paper on blockchain. The Hungarian DPA NAIH published an opinion before. It is available here http://naih.hu/files/Blockchain-Opinion-2018-01-29.pdf. The paper mostly addresses, who is controller and which DPA has supervision over them. The English version contains factual errors and inconsistent wordings. This might be due to translation errors. If I read it correctly, the NAIH treats all participants of a blockchain as controllers.*

Miners

Although miners are not regarded as controllers, the CNIL might regard them as processors. The CNIL is aware that this might constitute a problem for public blockchains and will discuss this further. The CNIL encourages the creation of contractual relations among the participants of a blockchain.

GDPR requires controllers to have a contractual arrangement with their processors and to control them. Public blockchains achieve the same purpose through blockchain software. Do we really need to add lots of contractual agreements that are technically not needed? Could we implement some kind of smart contract into blockchain software that defines the duties of processors and at the same time enforces these duties?

Avoid Blockchain if you can

The CNIL recommends blockchain not be used if it is not needed to achieve the desired purpose. The CNIL also recommends preference for permissioned blockchains because they allow control of where the data is processed. Permissioned blockchains can be combined with the known instruments that allow the transfer of personal data to countries outside the EU like binding corporate rules or standard contractual clauses.

From a technical point of view it also makes sense not to use blockchain if their features are not required. Although permissioned blockchains are a better match to the hierarchical model of responsibility of the GDPR, they often create another powerful intermediary and do not deliver the security, disintermediation and user empowerment that the blockchain usually stands for.

Public IDs on a Blockchain

The CNIL states that every blockchain has one public ID for every participant. From that they conclude that no further data minimization is possible.

This assumption is simply wrong. Unique public IDs are simply not required for blockchains. It is not even completely true for Bitcoin where people are advised to use multiple public IDs. It all depends on the type of blockchain you use.

Personal Data on a Blockchain

In order to minimize the impact on the data subjects, the CNIL sees an obligation to store the data in the format that reduces this impact. The CNIL sets an order of preference:

1. Zero knowledge proofs: The CNIL calls this “engagement cryptographic”. In a footnote this term is explained. The explanation covers zero knowledge proofs but could also include other techniques.
2. Peppered Hashing: The CNIL uses the phrase “hashage à clé”, which means to include a secret key when applying the cryptographic hashing function. In order to verify the hashed object with the hash value on the chain, the secret key – also called pepper – is needed. Peppered hashes are similar to salted hashes. However with peppered hashes the key is secret and is not the same for all objects. The additional key is important in the case that the hashed object is not secret or does not contain enough entropy, meaning that it could be guessed.
3. Encryption.
4. Hashing without pepper: If none of the above is possible, the purpose of the processing justifies this and a data protection impact assessment (DPIA) verifies that the risks for

the data subjects are acceptable. In this case, the personal data might also be stored as a hash without pepper (secret key) or even in clear text.

This order of technologies can be quite helpful for blockchain projects. However, I do not agree with the CNIL that hashing without a secret key is generally inferior to encryption. There are a list of projects where, for example, the hashed objects have enough entropy for guessing them to not be possible. If the hashed objects are secret then an additional secret key provides little additional security. While the interpretation of the GDPR by DPAs like the CNIL is not binding, the DPAs have the power to demand a DPIA (Art. 35.4). This means that anybody subject to oversight of the CNIL who puts hashed personal data or clear text personal data on blockchains needs to perform a DPIA.

Erasure of Personal Data

In its paper on anonymization techniques (05/2014, 0829/14/EN WP216), the WP29 was quite strict on what constitutes personal data – far stricter than recital 26 of the GDPR. The CNIL seems to soften this a bit. The CNIL acknowledges that there can be perfect cryptographic techniques for which deletion of a key equals the deletion of the data. For other techniques, rendering the personal data practically inaccessible might be considered as being close to deleting it.

The CNIL is not explicitly stating the legal consequences of being considered close to deletion. Do they still see it as processing of personal data but with practically a zero risk to the data subject? Does the overhead of GDPR including the duty to inform the data subject, record of processing activities etc. still apply for data where nobody has the ability to decipher it?

Rights of the data subject compatible with the blockchain

The CNIL sees no specific problem with complying with the rights of the data subject to information, including the right to data portability.

Governance

The CNIL recommends the creation of a contingency plan and a governance procedure to act on security issues.

Storage of Private Keys

The owner of a private key is considered a controller and has the duty to store their private keys in a secure manner.

The author, Jörn Erbguth, is consultant on blockchain, smart contracts and data protection
joern@erbguth.ch
https://erbguth.ch
https://www.linkedin.com/in/jorn-erbguth/