BLOCKCHAIN AND PERSONAL DATA PROTECTION

JPM | PARTNERS

Blockchain and Personal Data Protection
Publisher: JPM | Partners
Delta House, 8a Vladimira Popovića street
www.jpm.law
Authors: Ivan Milošević, Partner, Katarina Savić, Senior Associate
Design and prepress: JPM | Partners

Disclaimer:
The sole purpose of this publication is to provide information about specific topics.
It makes no claims to completeness and does not constitute legal advice.
The information it contains is no substitute for specific legal advice.
If you have any queries regarding the issues raised or other legal topics, please get in touch with your usual contact at JPM & Partners.

We are facing a remarkable growth of blockchain technologies. One of the main functionalities of this technology is to ensure the confidentiality, integrity, and availability of (personal) data.

This article addresses possible advantages and risks for the protection of privacy and personal data posed by blockchain technologies and manners how to mitigate risks to protect the rights and freedoms of data subjects and other natural persons. Achieving compliance with the Law on Protection of Personal Data in the context of blockchain principles requires a synergy of experts possessing technical, legal, and organizational skills.

Blockchain is a decentralized and reliable database ensuring transaction immutability. However, there are two sides to every coin - both the functionality of a product and compliance with the regulatory requirements must be implemented. The purpose of the Law on Personal Data Protection (“Law”) is to protect the privacy and personal data of individuals.

One of the main advantages of blockchain is that it belongs to a category of technology where a one-size-fits-all approach cannot be applied. There are various types of blockchain technologies, designed for different purposes such as cryptocurrencies, intellectual property, smart contracts, etc. This diversity requires a customized approach when assessing the compatibility of blockchain with the Law.

Blockchain Technology vs. Data Security

Blockchain is composed of blocks that are linked together in chronological order, forming a chain (chain of blocks). Each block in the blockchain contains a unique cryptographic hash of the previous block. Blocks are permanently connected and transactions are recorded sequentially.

From a security aspect, blockchain transactions are immutable and the (personal) data stored in a block cannot be altered retroactively by adversaries without altering all subsequent blocks. Multiply network participants collaborate to validate and record transactions, ensuring that no single entity from the security aspect has exclusive control over the system.

Immutability is considered to be one of the core characteristics and benefits of blockchain technology. It means that once data is recorded on the blockchain, it would be difficult for adversaries to rectify, alter, or erase them. This is achieved through cryptographic hashing, making it extremely difficult to modify the data. The purpose of this technique is to record financial transactions and other data preventing unauthorized subsequent rectifications.

Furthermore, blockchain is a technology based on a decentralized network of nodes. The concept of decentralization entails the absence of a central authority or intermediary meaning that only controllers can have control over personal data.

Minimisation Principle

In accordance with the Law, personal data shall be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. In the blockchain, all participating nodes store a copy of the entire ledger.

This can lead to the storage, i.e., processing of a significant amount of personal data that may not be directly relevant to a specific transaction - may not be relevant for the processing of a specific controller which further may violate the data minimization principle.

The breach of the data minimisation principle can be established by raising awareness of the controllers who use blockchain technologies.

Data Protection Impact Assessment

To address the requirements of the Law for the confidentiality of the data in blockchain nodes it is necessary to assess the risk of the resilience of the hash function to collision attack. Having that in mind, it is of utmost importance to choose a trustworthy provider of blockchain applications.

For addressing the said risks that may arise when it comes to different blockchain technologies, a Data Protection Impact Assessment (“DPIA”) would be considered advisable.

DPIA is a risk assessment of the impact of the processing operations on the rights and freedoms of citizens and shall be carried out when a type of processing is likely to result in a high risk to the rights and freedoms of natural persons, especially by using new technologies. Its purpose is to identify risks associated with the rights and freedoms of data subjects and other natural persons and shall result in defining adequate technical, organisational, and legal measures aimed to mitigate risks to an acceptable level.

Conclusion

While blockchain technology offers numerous advantages, it also poses challenges in ensuring data privacy and compliance with the Law. By conducting DPIAs and customizing strategies for each blockchain, organizations can achieve a balance between harnessing the potential of blockchain and respecting individuals' data protection rights.

Each blockchain is unique, and its structure and purpose may vary. Therefore, it is essential to conduct DPIA for each blockchain technology to determine compliance with the Law. This assessment should identify potential risks, recommend necessary changes, and guide the blockchain towards compliance with the Law.

Authors

Ivan Milošević

Partner

E: ivan.milosevic@jpm.law

Katarina Savić

Senior Associate

E: katarina.savic@jpm.law

JPM | PARTNERS
8a Vladimira Popovića,
DELTA HOUSE, V Floor
11070 Belgrade, Serbia
T:+ 381/11/207-6850
E: office@jpm.law

www.jpm.law