Proskauer

Blockchain, Personal Data and the GDPR Right to be Forgotten

Blockchain and the Law Blog on **April 17, 2018**

The effective date of the EU's General Data Protection Regulation (GDPR) is fast approaching (May 25, 2018), and its impacts are already being felt across various industries. Specifically, the conflicts between the GDPR and the technical realities of blockchains raise important legal considerations for companies seeking to implement blockchain solutions that involve the personal data of EU data subjects.

One of the key features of blockchain technology is the general immutability of its data, and many applications of the technology thus far are built on publicly available data trails. Among other data, a blockchain can house the information of those who have engaged in transactions along the life of the blockchain, whether it is their name or social security number or, more often, simply a code which could make an individual identifiable. Personal data in an immutable data trail is problematic when considered against the new requirements of the GDPR.

One issue that will have to be considered is the GDPR's "erasure" right. Article 17 of the GDPR demands that companies erase the personal data of individuals when they request to be "forgotten". The GDPR does not define what "erasure of data" means, which suggests that, to comply with this requirement, actual physical and logical deletion (a literal reading of the word "erase") is required. As simply conducting a blockchain transaction to make personal information inaccessible does not erase any data, it is not clear whether and how one can store personal data on a blockchain and comply with a literal reading of this GDPR obligation. Further complicating the matter is the fact that Article 4 of the GDPR defines "personal data" very broadly as any information relating to an identified or identifiable natural person, with "identifiable natural person" being defined to mean an individual who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location number, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Some practitioners and scholars believe that even an individual's publicly available cryptocurrency wallet address would be considered personal data under the GDPR.

One potential solution to this conundrum might be to store all personal data off of the blockchain in separate "off-chain" databases, but to do so would sacrifice many of the benefits of using a blockchain in the first place.

Until we have some clarification on the interpretation of the obligation to "erase" data, or until the GDPR is amended to account for the unique technical structure of blockchains, companies should be aware of the risk in developing blockchains that will include personal data of EU based individuals. While clearly an issue, as with much of the GDPR, a practical approach to compliance is recommended, and this is not likely to be the issue that is immediately put into play by complainants under the GDPR.

For general insights on the GDPR's various privacy and data security implications, please visit our Privacy Law Blog.

View Original