BakerHostetler

Brief

Five Things Blockchain Companies Need to Know About the GDPR

We are witnessing the convergence, and perhaps the collision, of two powerful new forces in data privacy: the European Union General Data Protection Regulation (GDPR) and the emergence of blockchain-based privacy solutions. As blockchain technology firms continue to build new solutions, here are five key takeaways they should keep in mind about the GDPR.

Personal Data

The GDPR applies to "personal data," which is defined as "any information relating to an identified or identifiable natural person ('data subject')." A "data subject" is a "natural person … who can be identified … by reference to an identifier … specific to the … cultural or social identity of that natural person." Moreover, personal data explicitly includes "online identifier[s]," including IP address.

1 Essentially, almost any piece of data that can assist in learning something about someone is likely to be considered personal data.

Under the GDPR, personal data even includes data that has undergone "pseudonymization," meaning that the data has been processed such that it "can no longer be attributed to a specific data subject without the use of additional information." Encryption is considered to be a highly effective means of pseudonymization, and "public keys" on a blockchain, which are associated with off-chain personal data, are also likely to be considered pseudonymized. While the GDPR prefers encrypting data to achieve pseudonymization, that encryption alone does not remove the underlying data from the definition of personal data and, therefore, does not serve to avoid GDPR requirements.

2 If personal data stored off-chain can easily be connected to a public key used in a blockchain solution, the public key is very likely to be considered data that has achieved a state of pseudonymization but is still regulated as personal data subject to the GDPR.

Where personal data has been pseudonymized and the additional information needed to attribute the data to a natural person is "not available," the GDPR indicates that the data may be considered "anonymous information" or "rendered anonymous." Because the GDPR only regulates personal data, anything considered anonymous is thus exempt from the GDPR, which "does not … concern the processing of such anonymous information …."

This provision suggests a path to conform blockchain solutions with the GDPR: If the blockchain architecture is designed such that public keys fit within the definition of anonymous information – by ensuring that any off-chain personal data is securely encrypted, and decryption is not available to permit reassociation with the public key – processing of public keys may be exempt from the GDPR's requirements, including the right of erasure.

This approach is consistent with recent guidance released by France's data protection authority, the Commission Nationale de l'Informatique et des Libertés (CNIL). The CNIL acknowledged that public keys are central to the "very architecture" of the blockchain, and therefore minimization of any other identifiers – whether through encryption, hashing or storage of personal data off-chain – is crucial.

3 Preserving the anonymity of public keys and minimizing identifiable information through privacy by design are arguably the most critical issues of concern for any company leveraging blockchain technology and dealing with personal data.

Controller vs. Processor

Entities subject to the GDPR have different obligations based on whether they are deemed a "controller" or a "processor" of personal data. In general, a controller "determines the purposes and means of the processing of personal data," while a processor "processes personal data on behalf of the controller."

The determination of whether an entity acts as a controller or a processor is activity-specific, not entity-specific. This means that, in different contexts, the same entity may be deemed a controller, a processor, or both a controller and

processor. Controllers, as the entities determining the means and purposes of the processing, have significantly more obligations under the GDPR than do Processors. Most importantly, controllers have the responsibility for implementing requests from individuals who want their personal data deleted, amended or transferred.

4 Companies leveraging blockchain technology should design their systems so that they avoid determining how and why data is processed, and thus avoid being deemed a data Controller.

The Rights of Data Subjects and the Lawful Basis of Processing Data

The GDPR gives data subjects various rights with respect to controllers of their data. Chief among these are the rights to data portability (i.e., the right to take your data with you), rectification (i.e., the right to amend any incorrect data) and erasure (i.e., the right to be forgotten). In general, these rights can be exercised at the request of the data subject, although there are exceptions to some rights in certain cases, such as when the data is being processed or retained pursuant to a legal obligation.

The obligations of data controllers to facilitate data subjects' rights vary based on the lawful basis under which the data is processed. The processing of EU personal data must be supported by one of six legal bases, according to the purpose of the processing. These bases are:

- **Consent.** Consent by the data subject to one or more specific purposes.
- **Contract.** Necessary for the performance of a contract.
- **Legal obligation.** Necessary for compliance with a legal obligation to which the data controller is subject.
- **Public interest.** Necessary for the performance of a task carried out in the public interest.
- **Vital interests.** Necessary for the protection of the vital interests of the data subject.
- **Legitimate interests.** Necessary for the legitimate interests of the controller or a third party unless overridden by the fundamental rights and freedoms of the data subject.

Because consent may be withdrawn at any time, requiring deletion of any personal data collected on the basis of that consent, it is not an advisable or reliable basis for processing personal data that will be entered onto a blockchain. Similarly, while personal data may be collected and processed pursuant to the performance of a contract, if that contract is terminated or expires, the lawful basis for processing ends and the data must be deleted. On the other hand, data collected to comply with a legal obligation is likely exempt from the right of erasure. In the event that a data subject requests deletion of personal data on the blockchain, however, the CNIL has suggested that destruction of the underlying keys or information may be sufficient to "approximate the effects of erasure."

5 Understanding the applicable lawful basis or bases for processing data – especially any applicable limitations or exceptions to data subject rights under that basis – and designing your system accordingly are critical to building GDPR-compliant blockchain solutions.

Avoiding a Collision

Ultimately, whether these two forces are on a collision course has yet to be determined. Avoiding a collision will require some favorable interpretations by EU regulators to ensure that the GDPR does not deprive the EU and EU data subjects of the benefits offered by blockchain technology.

While the CNIL's guidance acknowledged the inextricable relationship between public keys and the blockchain, a clear determination by EU officials that public keys used in appropriately designed blockchain solutions do not themselves constitute personal data would go a long way toward reconciling blockchain technology with the GDPR.

Even if such a determination is made, users of blockchain solutions should monitor whether technological developments, specifically in data storage or encryption, would affect or change such a determination. At this critical moment, it is imperative that blockchain firms understand the GDPR's framework and take a proactive stance, developing technologies and legal positions that carefully account for the GDPR's requirements.

As these two powerful forces continue to emerge and take effect, EU regulators and blockchain technologists alike would do well to remember that the GDPR and blockchain-based solutions share many fundamental goals, such as the right of individuals to control their own data and the minimization of data sharing. To demonstrate the compatibility of blockchains and the GDPR, these principles should be leveraged to the greatest extent possible in blockchain solution architectures.

The Final Word

With the right technical architecture and legal analysis, companies can harness the benefits of a blockchain while ensuring that data stored on a blockchain is compliant with GDPR requirements.

Originally published by BTC Media LLC in *Bitcoin Magazine*.

Contacts

Laura Jehl
+1.202.861.1588
ljehl@bakerlaw.com

Robert Musiala
+1.312.416.8192
rmusiala@bakerlaw.com

bakerlaw.com

Recognized as one of the top firms for client service, BakerHostetler is a leading national law firm that helps clients around the world address their most complex and critical business and regulatory issues. With five core national practice groups – Business, Employment, Intellectual Property, Litigation and Tax – the firm has more than 940 lawyers located in 14 offices coast to coast. For more information, visit bakerlaw.com.

22.10.18.11.24_p00