Blockchain and the GDPR: Threading the Needle

By Laura E. Jehl, Robert A. Musiala Jr. and Stephanie N. Malaska

Historically, regulation has tended to chase new technologies, lagging behind groundbreaking developments and often cramming them awkwardly into existing frameworks of applicable law. This year, however, new regulation is coinciding with the advent of new technologies. We’re 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. These two forces share similar fundamental principles, such as individual control over personal information and data minimization, and blockchain may very well offer simple and powerful solutions to implement some of the GDPR’s mandates. At the same time, these two forces – which have emerged independently – are on a potential collision course, particularly with respect to the GDPR’s right to erasure, also known as the “right to be forgotten.” Blockchain technology, when used for digital identity solutions, offers individuals unprecedented control over the ways their personal data is shared and used; but the immutable nature of the blockchain’s decentralized ledger appears to fundamentally clash with the GDPR’s mandate that personal data must be capable of being altered or deleted at the request of the individual to whom that data pertains. Once data is entered onto a blockchain, it can never be changed and it will never disappear.

This conflict between the GDPR and blockchain-based approaches to data privacy is rooted in two fundamentally different philosophies about how best to protect data privacy. The EU’s vision, codified in the GDPR, views centralized, governmental authority as essential to protecting consumers and their information against the abuses of private actors, particularly hulking, data-driven technology companies. By contrast, blockchain identity solutions arose out of bitcoin’s crypto-libertarian ethos, which scorns centralized authority and believes that privacy rights are best protected not by human institutions but by advanced cryptography and distributed networks that no single actor can control. The GDPR in some ways seeks to enhance personal privacy by reordering and further consolidating the balance of power in a familiar paradigm, while blockchain seeks to achieve the same goal by changing the paradigm completely. These foundationally different approaches result in some fundamental inconsistencies of form – but not necessarily of substance – in their two paths to solving the same problem.

Although blockchain developers have reason to be nervous, or at least very vigilant, about GDPR compliance, we believe that the GDPR does not preclude businesses engaged in processing EU personal data from using blockchain. Instead, it requires those businesses to be meticulous in the architecture of their blockchain systems to ensure that the data they record on a blockchain is not considered “personal data” subject to GDPR requirements. In particular, businesses should pay close attention to how public keys might be treated and classified under the GDPR’s framework. Because the GDPR’s definition of “personal data” extends to anything that can be traced back to an identifiable person, including IP addresses, a unique public key or address on the blockchain potentially falls within a regulatory gray area. Public keys were not specifically considered during the drafting of the GDPR, and their status is likely to be a subject of evolving interpretation with high-stakes consequences for companies working with blockchain solutions.

If the architecture of a blockchain solution relies on the storage of personal data on a blockchain, the solution will be incompatible with the GDPR and its requirements that such data be alterable or erasable. If EU personal data is entered onto a blockchain – even inadvert-
tently—it cannot be removed, leaving the developers potentially exposed to the Thor hammer of the GDPR’s penalties and perhaps dooming that particular blockchain solution. However, if a blockchain solution is carefully designed with the GDPR in mind, with only public keys stored on chain and with any off-chain personal data securely encrypted and unavailable to the blockchain developer, strong arguments can be made that the GDPR’s rights of erasure, rectification and data portability are not implicated.

**What Blockchain Firms Need to Know 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” [GDPR Art. 4(1)]. Moreover, personal data explicitly includes “online identifier[s],” including IP addresses.

The Takeaway: *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” [GDPR Art. 4(5)]. 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.

The Takeaway: *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 regulates only personal data, anything considered anonymous is thus exempt from the GDPR, which “does not . . . concern the processing of such anonymous information” [GDPR Recital 26]. 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 re-association with the public key—processing of public keys may be exempt from the GDPR’s requirements, including the right of erasure.

The Takeaway: *Preserving the ability to have public keys deemed anonymous under the GDPR is arguably the most critical issue of concern for any company leveraging blockchain 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 “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” [GDPR Art. 4(7), (8)].

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 important, Controllers have responsibility for implementing requests from individuals who want their personal data deleted, amended or transferred.

The Takeaway: *Companies leveraging blockchain 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 [GDPR Art. 6(1)]. 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.

**The Takeaway: 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.**

**Threading the Needle**

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. A decision 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 blockchain and the GDPR, these principles should be leveraged to the greatest extent possible in blockchain solution architecture.

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

**Author’s Information** Laura Jehl is a partner at BakerHostetler based in Washington, D.C. She is co-leader of the firm’s General Data Protection Regulation (GDPR) and Blockchain Technologies and Digital Currencies initiatives.

Robert Musiala is counsel at BakerHostetler based in Chicago where he advises blockchain industry clients on strategies for mitigating personal and business risk and achieving regulatory compliance.

Stephanie Malaska is an associate at BakerHostetler based in Washington, D.C. Her practice includes advising companies on data privacy, including GDPR, and on blockchain and other emerging technologies.

The views expressed in this article are those of the authors and not necessarily those of BakerHostetler or its clients, or of Bloomberg Law.