How Blockchains May Comply With GDPR Mandates: Part 2

By **Kennedy Luvai** (May 3, 2018)

Kennedy Luvai

The first half of this two-part article explored how the European Union’s General Data Protection Regulation, enacted to provide enhanced privacy rights to EU residents against a siloed, centralized data storage framework, may present some challenges to certain blockchain-based solutions. Specifically, the article examined that the treatment of unreadable hashed or encrypted data as pseudonymous data, subject to the GDPR, may have far-reaching implications that extend beyond the right to erasure mandate. In the following article, we will consider additional implications of the GDPR, including the rights to data minimization, to rectification of inaccurate data, access to data and access to data portability.

Additional Brief Primer on the Types of Blockchains

There is no single type or model of distributed ledgers or blockchains. Whether a blockchain solution may comply with the various GDPR privacy mandates (including the previously discussed erasure mandate) depends on the nature of the blockchain upon which the solution is built — private blockchains versus public blockchains and permissioned blockchains versus nonpermissioned blockchains.

Anyone may participate in the network of a public blockchain, which typically incorporates mechanisms to incentivize participating nodes to join.[1] Public blockchains are typically set up as nonpermissioned blockchains where the participating node need not obtain permission from any person or entity in order to join and participate in the network. Besides bitcoin, the ethereum blockchain is another example of a popular public nonpermissioned blockchain.

In contrast, a private blockchain requires an invitation for a participating node to join. The node must be approved by either the company or consortium responsible for setting the system operation rules or be based on a set of rules set forth by the entity or consortium. Entities that establish private blockchains typically set them up as permissioned blockchains where participating nodes are subject to restrictions as to whether they may participate in the network, and how. Usually, some relationship exists between the entity responsible for system operation and each participating node. Ripple and Hyperledger Fabric are examples of private permissioned blockchains.

The Type of Blockchain Used May Impact the Designation or Identification of Data Controllers

Due to GDPR obligations imposed on companies that collect personal EU residents’ data for commercial purposes, identifying the data controller in a blockchain network subject to such obligations is key. A data controller is the natural or legal person, public, authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.[2] Identification may be impacted by the nature of the blockchain.

From a GDPR perspective, either no node from a public nonpermissioned blockchain qualifies as a data controller, or all of the nodes qualify as data controllers. If no node qualifies as a data controller, the blockchain solution cannot comply with the GDPR. Alternately, considering all nodes as data controllers raises complications including the following: (1) It may be difficult for an EU resident to identify and contact the person or entity running any particular node in order to exercise their rights granted by the GDPR,[3] (2) The node is likely to have access only to an unreadable hashed or encrypted copy of the ledger thus making it impossible to act on any request from a data subject. Any personal data from EU residents in any form. readable, hashed or encrypted — saved to a public nonpermissioned blockchain, would likely violate the GDPR.

The necessity of companies or consortia to set the rules of system operation in private permissioned blockchains has been criticized by some as introducing the very centralization that blockchain systems seek to avoid. Nevertheless, the introduction of such centralization agents may make it possible for private permissioned blockchains to be GDPR-compliant. The governance arrangement may impact or dictate how the stakeholders in the private permissioned blockchain may share the obligations imposed under the GDPR, i.e., whether the company or consortium solely determines the purposes and means of processing of the data (as a data controller) or whether it does so jointly with a participating node (as a joint controller with one or more of the participating nodes).

Implications of Other Additional Mandates on GDPR Compliance

Data Minimization

Article 25 of the GDPR mandates that "[t]he controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility." This mandate has interesting implications with regard to blockchains given that they are, by design, ledgers that grow with time and are replicated across multiple nodes.

The design feature that results in tamper-proof blockchain ledgers does complicate compliance with the data minimization mandate. The selected approaches discussed in the context of the erasure mandate may be available to address the data minimization concern for any personal data found in a blockchain. Thus, to the extent it is feasible, the editing of an otherwise "immutable" permissioned blockchain using the chameleon hash function may be an option. Alternatively, personal data stored on an off-chain database may be modified and minimized while leaving pseudonymized data — unreadable encrypted or hashed personal data — on the blockchain. As previously discussed, whether the corresponding unreadable encrypted data or hashed data reference is deemed to be functionally erased depends on the various data protection authorities' views on whether the pseudonymization of data may, in certain cases, satisfy the erasure mandate.

Erasure or Rectification of Inaccurate Personal Data

Article 5 of the GDPR provides that personal data collected shall be "accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate … are erased or rectified without delay." The GDPR then mandates, in Article 16, that the "data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate data concerning him or her" and taking into account the purposes of the processing, "[t]he data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement."

Setting aside the complications inherent in a public nonpermissioned blockchain architecture, assuming that all nodes are data controllers, it is unlikely that any single node, acting as a data controller, would be able to fulfill this obligation by effecting an erasure or rectification of inaccurate personal data. In all likelihood, that node would not itself have access to a readable version of personal data.

Alternately, and depending on the nature of the solution based on a private permissioned blockchain architecture, there may be ways to comply with this mandate. The considerations relevant to the erasure component have been previously discussed.[4] As to rectification, where personal data is stored off-chain with unreadable hashed or encrypted references on the blockchain, the correction of the inaccurate personal data may take various forms including, among other means, correcting the off-chain personal data and then editing the otherwise "immutable" blockchain as discussed in the companion article, or correcting the off-chain database by adding new or missing information and adding new data to new blocks to be added to the blockchain.

Access to Personal Data

Article 15 of the GDPR establishes a robust right to access where an EU resident may obtain confirmation from the controller that his or her personal data is being processed as well as among other information, the purpose for the processing, the categories of the personal data concerned, recipients or categories of recipients of the personal data and information pertinent to the period of time to which the personal data will be stored. This article also provides that the data controller "shall provide a copy of the personal data undergoing processing."

Article 15 raises questions of whether solutions built on public nonpermissioned blockchains to which personal data is saved, even in unreadable hashed or encrypted forms, could be GDPR-compliant.[5] Participating nodes typically have access to the unreadable hashed or encrypted data and would not ordinarily be in a position to provide confirmation of whether or not a particular data subject's personal data or related information is being processed or be able to provide a copy of the personal data being processed.

To the extent that one is dealing with a solution built on a private permissioned blockchain in which the readable personal data is stored off-chain with only a hashed or encrypted reference of that personal data to the blockchain, it appears that it may be possible to comply with the GDPR. In such a setting, the data controller[6] may, depending upon how the blockchain solution is structured, be able provide the kind of confirmation and additional information envisaged under Article 15. Also, given that the personal data of the requesting data subject would be stored in an off-chain database, such a setting would permit the data controller to provide a copy of the personal data undergoing processing.

Portability of Personal Data

As a response to the "big data" trends and in addition to the right of access, the GDPR creates a new right, under Article 20, to data portability that seeks to increase user choice with regard to online service offerings.

Where the data processing is carried out by "automated means" and based on either the data subject's contractual agreement or consent, the data subject shall have the right to obtain the personal data he or she has provided to the data controller "in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided." Article 20 further provides that "where technically feasible," the data subject shall have the right to have personal data transmitted directly from one controller to another.[7]

As with the right-to-access discussion above, the same considerations regarding the likely noncompliance of public nonpermissioned blockchain solutions where personal data is saved to the blockchain are in play. The same discussion holds true as it relates to the possibility that private permissioned blockchain solutions, depending on how they are set up, may be GDPR-compliant with the additional wrinkle that the personal data stored off-chain should be provided to the data subject or the destination controller in a "structured, commonly used and machine-readable format."

Use of Private Permissioned Blockchains May Provide Flexibility to Structure Solutions that are GDPR-Compliant

There is no single model for blockchains — they range from public nonpermissioned blockchains to private permissioned blockchains. Because the GDPR, as enacted, is designed to work in a more or less centralized data privacy universe, solutions built upon private permissioned blockchains incorporating a measure of centralization may be structured to comply with the spirit, if not the letter, of the regulation. The same does not necessarily hold true of solutions built on public nonpermissioned blockchains. Companies building solutions on public nonpermissioned blockchains may avoid potential liability under the GDPR only by ensuring that no personal data (encrypted, hashed, or otherwise) belonging to EU residents appears on the blockchain.

Kennedy K. Luvai is a shareholder at Parsons Behle & Latimer PLC in Salt Lake City, and a former software developer.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] In the Bitcoin blockchain, for example, the incentive for nodes to participate in validating transactions through the solution of arbitrarily complex mathematical problems is the chance to earn new bitcoin.

[2] The concept of data controller was briefly introduced in the companion article, How Blockchains May Comply with GDPR's Erasure Mandate.

[3] This raises the question of how the various supervisory authorities in the EU would enforce the mandates of the GDPR or levy penalties against individual or entities operating participating nodes that may be difficult to unmask and, even if they are identified, may be dispersed across the globe thus complicating any enforcement activities.

[4] Considerations pertinent to the erasure of personal data was the focus of the companion article identified above.

[5] This assumes that each participating node is deemed to be a data controller in such a setting.

[6] As determined either by the company or consortium responsible for system operation or by the rules relating to the governance of the blockchain.

[7] Incidentally, this could entail a company having to transmit that personal data in a "structured, commonly used and machine-readable format" to one of its competitors.