CEP Magazine - August 2020
Blockchain and the GDPR: Can the conflicts be resolved?

By Melanie Brown

Melanie Brown (m.brown@blackdogrisk.com) is a Regulatory Compliance Attorney and President and Consultant for Black Dog Risk Solutions LLC in Rio Rancho, New Mexico, USA.

Innovating processes, procedures, and performance can make a significant impact on compliance initiatives. By incorporating technology in a compliance program, a business can increase efficiency, applicability, reliability, and, overall, corporate responsibility. This article will explain the concept of "blockchain" and consider the implications of recent privacy law developments such as the European Union (EU) General Data Protection Regulation[1] (GDPR) on the use of blockchain technology.

What is blockchain?

One technological advancement that can positively affect an internal compliance program is the use of blockchain technology. For non-techies, blockchain is distributed ledger technology that digitally stores or moves data between parties to a business transaction. Putting it simply, blockchain securely records each new transaction or data to a ledger. As new transactions occur, they are stored in a "block." The sequencing of the transactions grows as each additional transaction occurs, creating an irreversible and immutable "chain," ergo, blockchain.

Blockchain is an immutable and irreversible distributed ledger because all data or transactions recorded to the ledger cannot be changed, amended, or edited. Therefore, when parties make modifications to data or transactions, they will be appended to the chain. Certain known or identified parties to the transaction are invited to private blockchains to access transaction information, or in some cases, the transactions are public blockchains, where transactions are decentralized and parties have little to no knowledge of each other. Blockchain uses public and private encryption keys to protect the integrity of the transaction data, manage party access, and provide transparency.[2]

Blockchain is being used in several industries. From the retail to the music industry, companies are implementing blockchain. It reduces time and money by eliminating the use of third-party middlemen and increases security with the use of encryption. The transactions are distributed smoothly among parties.

How is blockchain associated with an internal compliance program, and what complications does it create? Well, consider this:

- In a global company that imports and exports, international trade law and US federal law require a series of steps to comply with regulations. To ensure these steps are appropriately taken, the transaction can be added to the blockchain. For example, the import/export industry is still heavily paper driven. Shipments, certifications, and clearance processes that require a paper trail can be digitally driven in blockchain.

- In a financial audit, due to federal regulations like the Sarbanes-Oxley Act[3] (SOX), the audit process could be maintained in blockchain as an electronic paper trail. The blockchain would securely record each document, errors, and conclusions as part of the audit. It can also provide transparency in real time.

Because blockchains are highly secured, they could potentially meet the security standards of auditing requirements. Blockchains could also facilitate SOX sections 302 (Corporate responsibility for financial reports), 404 (Management assessment of internal controls), and 409 (Real time issue disclosures).

- During contract negotiations, compliance personnel want to ensure that certain terms and conditions are included in the final contract. The various versions of the contract can be included in blockchain. Each new revision is a new transaction to the chain. The blockchain tracks which party accesses the contract and what changes were made when the edited version is placed on-chain. Final execution of the contract is memorialized by the signatures stored to the blockchain.

Blockchain can be used in other areas that require compliance, such as supply chain, recordkeeping, and even the onboarding of new employees.

Blockchain versus the GDPR?

There are, however, some restrictions that occur with the use of blockchain technology. One of those restrictions is compliance with privacy and data protection laws. Currently, it's arguable that blockchain is not compliant with GDPR.

At this point, most compliance professionals are familiar with the GDPR. The GDPR is a new regime of privacy protection promulgated by the European Parliament and the Council affecting the EU and the European Economic Area. The GDPR replaced the 1995 Data Protection Directive of the EU, which was the primary law that governed the processing and movement of personal data. The GDPR was adopted in 2016 and became binding in 2018.[4]

There are mainly two objectives of the GDPR. First, it attempts to enable the free movement of personal data between the EU's member states. Second, it establishes a framework of fundamental rights protections to personal data of data subjects or "natural persons" of the EU and data subjects that are based in the EU (herein individuals). The free movement of personal data means the "processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system."[5]

There are exceptions to what is considered "processing" of personal data. One of those exceptions is processing activities "by a natural person in the course of a purely personal or household activity." This specific issue came to the forefront of the general discussion of the scope and enforcement of the GDPR when a Dutch grandmother was found in violation of the GDPR in the Netherlands this year. In this case, the grandmother had posted photos of her grandchildren on Facebook and Pinterest, at the objection of the children's mother. The court found that even though the GDPR does not apply to a "household" exception, because the photos were posted on the internet via social media that was available to an indefinite amount of people, the GDPR applied.[6]

The processing of personal data means the collection, recording, and storage of personal data. Pursuant to the GDPR, the processing operations are assigned and conducted by controllers (the natural or legal person, public authority, agency, or other body that, alone or jointly with others, determines the purposes and means for processing personal data) and processors (a natural or legal person, public authority, agency, or other body that processes personal data on behalf of the controller).[7] Data controllers are required to protect accuracy, storage, and the confidentiality of personal data, while data processors are chosen by the data controller to process the data.

Compliance and recognition of data subject individual rights

There are various areas of the GDPR that call into question blockchain's ability to comply. One area that is worth mentioning is noncompliance with a data subject's individual rights. Chapter three of the GDPR includes eight individual rights for a data subject. As mentioned above, compliance by controllers and processors is paramount to the efficacy of the GDPR. Struggles with blockchain's compliance with some of the individual rights is affected by the roles of controllers and processors.

The right to be informed

Articles 13 and 14 of the GDPR grant individuals the right to be informed about the collection and use of their personal data.[8] This is a key transparency requirement under the GDPR. Individuals have a right to know the purposes for processing their personal data, retention periods for that personal data, and who it will be shared with. This information must be provided to individuals at the time their personal data are collected.

The first issue in implementing GDPR with blockchain is: Who is the data controller and processor to a blockchain? One of blockchain's benefits is its ability to decentralize the processing and storage of transactions and data across a wide range of parties. That being the case, it is often unclear which party determines the purposes and means of processing. This is affected by the private and public blockchains.

Private blockchains make it easier to identify controllers and processors because there is typically a central operator or group that likely could qualify as controller(s), assuming they have control over the blockchain that is organized by a company and have the ability to determine the purpose and means for processing the personal data. Public blockchains, by contrast, usually lack a central individual or consortium. Furthermore, multiple parties frequently process data or transactions on a blockchain. So, how practical is it that all the parties are processors?

Without the ability to identify a clear controller or processor, it is unclear who the individual would or could approach to exercise their right to be informed.

The right to access and right to rectification

Under Article 15 of the GDPR, the right of access, commonly referred to as subject access, gives data subjects the right to obtain a copy of their personal data as well as other supplementary information. It helps them to understand how and why their data are being used and if the use is lawful. Individuals can make a written or verbal request to access their data, and the controller has up to 30 days to respond to the request.[9] There again, without the ability to identify a specific controller, who would an individual approach to exercise their right to access? Additionally, there can be many locations in blockchain where personal data are held because the transactions or data in blockchain get distributed to the parties who maintain the data on their computers. That would require all parties to comply with the right to access.

Not only do individuals have a right to access their personal data, the data have to be accurate, and if inaccurate, the individual has the right to have the data rectified. Furthermore, if the personal data is incomplete, the GDPR offers the data subject the right to complete incomplete information. Similar to the right to access, the request can be made verbally or in writing, and the controller has up to 30 days to respond to the request. Blockchains make it difficult for individuals to exercise their rights of access and rectification.

The right to erasure versus the right to restrict processing

Under Article 17 of the GDPR, individuals have the right to have personal data erased. This is also known as the "right to be forgotten." The right is not absolute and only applies in certain circumstances.[10] The

circumstances where the right is inapplicable are mostly for legal requirements, public policy, scientific research, preserving public health, and when the request is "manifestly unfounded." However, if those exceptions are inapplicable to blockchain data or transactions, the controller has to comply and erase the personal data under GDPR. But remember, if the data were part of a transaction in a blockchain, the chain is immutable and irreversible, so the data could not be erased, and therefore the blockchain becomes noncompliant with the GDPR.

What also makes compliance with this right onerous is that if personal data have been disclosed to others, each recipient must be contacted and informed of the request for erasure, unless this proves impossible or involves disproportionate effort. If asked to, the controller must also inform the data subjects about these recipients. The GDPR defines a "recipient" as a natural or legal person, public authority, agency, or other body to which the personal data are disclosed.[11] The definition includes controllers, processors, and persons who, under the direct authority of the controller or processor, are authorized to process personal data.

An alternative to the right to erasure is an individual's right to restrict or suppress the processing of their data, which, in certain circumstances, prevents the need to exercise their right to erasure. Individuals have the right to restrict the processing of their personal data where they have a particular reason for wanting the restriction. This may be because they have issues with the content of the information held or how their data have been used. In most cases, an individual's personal data cannot be restricted indefinitely, but the restriction will need to be in place for a certain period of time.

What you can do to use blockchain technology

Although every situation is different and requires specific analyses, here are some general recommendations:

1. Implement a private blockchain when available.
2. Identify a data controller and processor(s) before blockchain technology is implemented.
3. Execute a contract with the controller(s) and processor(s) before the implementation of blockchain.
4. Distribute policies and procedures useful in private and public blockchains so, even though the purpose is to be decentralized, such policies and procedures can be distributed and/or made available to all parties.
5. At the construction phase of blockchain, seek assistance and information from the developers themselves on how the chain will operate and what controls, if any, can be added.

Conclusion

If you are interested in innovating your compliance program, consider how to improve efficiency, applicability, reliability, and corporate responsibility through the use of blockchain, but be aware of the potential conflicts between its use and data protection laws such as the GDPR.

Takeaways

- Compliance professionals can enhance a compliance program's efficacy and efficiency through the use of blockchains.
- Blockchain is an unchangeable and an unalterable distributed ledger technology that eases the flow of transactions and data among parties with security and transparency.
- New privacy laws like the European Union General Data Protection Regulation (GDPR) present problems

for the use of blockchain.

- Compliance professionals can add policies and contracts on-chain to give notice to parties and promote compliance with the GDPR.
- Conferring and collaborating with blockchain developers can help compliance professionals facilitate compliance with privacy regulations.

1 Council Regulation 2016/679, General Data Protection Regulation, 2016 O.J. L119.
2 Jared R. Butcher and Claire M. Blakey, "Cybersecurity Tech Basics: Blockchain Technology Cyber Risks and Issues: Overview," *Practical Law*, w-017-1916, 2019, https://bit.ly/3dppi57.
3 Sarbanes-Oxley Act, Pub. L. No. 107-204, 116 Stat. 745 (2002).
4 Robbie Downing, "Overview of EU General Data Protection Regulation," *Practical Law*, w-007-9580, 2020, https://tmsnrt.rs/3eGUxZw.
5 Scientific Foresight Unit, *Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?* European Parliamentary Research Service, July 2019, https://bit.ly/3031sZj.
6 Matt Binder, "Grandma ordered to delete Facebook photos of grandkids or face fine," *Mashable*, May 22, 2020, https://bit.ly/3dmKhW9.
7 Information Commissioner's Office, "Key definitions: Controllers and processors," *Guide to the General Data Protection Regulation (GDPR)*, accessed June 1, 2020, https://bit.ly/2XTr8EK.
8 Information Commissioner's Office, "Individual rights: Right to be informed," *Guide to the General Data Protection Regulation (GDPR)*, accessed June 1, 2020, https://bit.ly/2U0O6bZ.
9 Information Commissioner's Office, "Individual rights: Right of access," *Guide to the General Data Protection Regulation (GDPR)*, accessed June 1, 2020, https://bit.ly/2BmYuo4.
10 Information Commissioner's Office, "Individual rights: Right to erasure," *Guide to the General Data Protection Regulation (GDPR)*, accessed June 1, 2020, https://bit.ly/36TCrBc.
11 Information Commissioner's Office, "Individual rights: Right to erasure."