Grant Thornton

GDPR & Blockchain

Blockchain solution to General Data Protection Regulation

Content

Understanding GDPR

Specific Distributed Ledger Technology (DLT) known as Blockchain has taken centre stage in all economic sectors due to its potential of transformation. The surrounding hype relates to blockchain's ability to disrupt the role of intermediaries in transactions, simplifying processes and creating new operating models and workflows.

This leads to deep cost reductions and potential increase of profits for companies operating within. Blockchain introduces features which have never been possible before, examples; immutability of transactions and other activities, and the decentralization of record keeping. These features, however, raise some legal and regulatory challenges in terms of data protection which should be addressed.

Addressing the Regulatory and Legal Challenges

As blockchain is still in the preliminary phase of the technology lifecycle, in many cases no concrete or shared approach has been accepted at an industry level in relation to the application of existing and incoming regulation.

However, a positive update is that public bodies such as the European Commission, and other regulators are rapidly catching up with the trending technology. This provides, at least foundation level indications as to how blockchain should be treated in relation to topics such as data protection and privacy. It also provides a sense of security for companies wishing to advance blockchain applications and use cases outside of the research labs.

This paper focuses on the challenges and advantages of blockchain in relation to GDPR implementation.

General Data Protection Regulation (GDPR)

The latest legislation created for EU member states in terms of data protection is GDPR, or regulation (EU) 2016/679. The remit of GDPR is broad; aiming to achieve the complete protection of natural persons in the EU with regard to the processing (including retainment) of personal data, and on the free movement and removal of such data from specified databases. It comes into force in May 2018.

What is GDPR replacing, and why?

Data protection regulation **directive 95/46 CE**, which retains its status until May 2018, had originally set out general data protection objectives which Member States were expected to comply with. However the **perceived weakness** of the former regulation could be viewed as the ability and freedom it gave Members States to articulate national legislation in isolation (provided that they comply with the general objectives set in the directive).

This freedom lead to differences and discrepancies amongst Member States in a way each chose to interpret and implement. The result was an inconsistency between countries, which, in many cases restricted operations in one single market (the EU). This inconsistency in the free movement of data (among other aspects) lead to obstructions within the European digital economy.

GDPR key Strengths

Alternate to the former, GDPR applies to the personal data of any natural person regardless of nationality or place of residence within the European Union (provided that requirements set in article 3 are complied with). Further, GDPR provides much deeper guidance of what is considered personal data, defined within - *as any information relating to an identified or identifiable natural person* - one who can be identified, directly or indirectly, in particular by reference to an identifier such as; *a name, an identification number, location data, 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.

GDPR´s Anonymization Techniques

This distinction between personal and non-personal data is of crucial importance, taking into account that information stored in blockchain is immutable, since non personal data falls out of scope of data protection legislation. In order to convert personal data into non-personal data and therefore not be subject to GDPR, it is necessary to apply anonymization techniques. These techniques consist of preventing identification of the holder of the data.

Leveraging Blockchain to achieve GDPR Compliance

1 **Lawfulness of processing (and the right of cancellation, erasure, and to be forgotten):** personal data processing shall be lawful when the data subject has given consent to the processing of his or her personal data. It shall be as easy to withdraw as to give consent.

Challenge: Implied by the requirement of removing personal data from the blockchain network in the event the data subject withdraws the consent.

2 **Accuracy principle (and the right of rectification):** personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

Challenge: There must exist a way to modify or alter the information stored on blockchain.

3 **Storage limitation:** personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

Challenge: Requires a method of future removal, when the purpose for which data were collected, has finished.

4 **Integrity and confidentiality:** personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

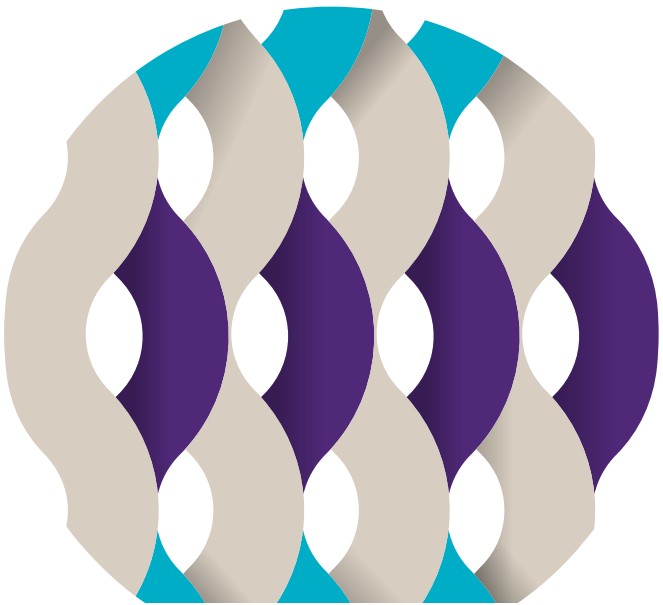
Challenge: All node participants in a blockchain network have access to data stored therein (blockchain is a decentralized network which implies that each node has a copy of each transaction), regardless of the consent of the data subject.

Solution – Grant Thornton Approach

Grant Thornton believes Blockchain technology solutions exist for the challenges presented by GDPR, making its principles compatible with the technology. These solutions can be divided into two groups: **Cryptographic Hashing** and **Private Channels** with encrypted data. Both are discussed below.

Cryptographic Hashing

Private channels



Blockchain Solution to GDPR Principles

Cryptographic Hashing

What is hashing?

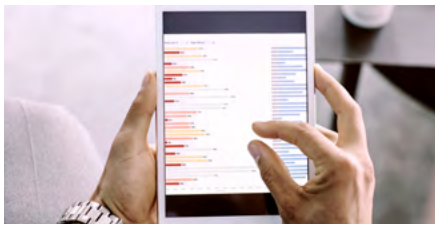
Hashing is a technique that consists of replacing one attribute (typically a unique attribute) in a record by another (a unique numerical identifier) using a hash function. When we refer to the term hashing in the digital world, it's usually referring to as a cryptographic hash. This is essentially the "fingerprint" of specific data. When processing personal data, a hash or identifier would be generated for each unit of personal data. The hash corresponding to each unit of personal data will be stored in the blockchain network while the unit itself will remain stored in a common external data base.

How does hashing solution work?

Data removal: When the personal data must be removed, according to principles of lawfulness of processing or storage limitation, the controller (company) removes the data from the external database, where the corresponding hash remains in the blockchain. Since the data related to this hash has been removed, the hash becomes a number with no correspondence, rendering the blockchain information scrambled or unreachable.

Data modification: In the event the data needs to be modified, according with accuracy principle, controller would effectively modify the record in question from the external data base. The updated record would replace the former in the external database and the updated record receives a new hash that will be stored in the blockchain. The previous hash corresponding to the former personal data is now a random number with no meaning without the corresponding (deleted) data.

Confidentiality: Since hashes are stored in the blockchain and personal data remain stored in a database outside the network, the participants in the blockchain network only would have access to the hashes, random numbers with no meaning for them, complying with integrity and confidentiality principle.



Further Protection: "Salted Hashes"

All solutions previously described are based on the assumption that hashing technique is a sufficient measure to ensure the removal of access to data on a blockchain, however there is one scenario which could serve to challenge the approach. Consider the following example:

If the range of hash codes being used by a company and the data contained in a database are known, all possibilities within the range could be entered on a trial and error basis until a ´forgotten´ record is reached. This may potentially involve ultimately considering a hash as a personal data, and therefore subject to GDPR. For this reason, it is necessary to reinforce hashes using a "salt". "Salt" is a random data that is used as an additional input to the attribute (personal data) being hashed. This reduces the likelihood of deriving the input value.

The usage of hashing function with salt is important in order to guarantee as much as possible the anonymization of the personal data in blockchain, especially when data are going to be removed and the hash remains in the blockchain indefinitely. In this regard, according to Opinion 5/2014 of Article 29 Working Party, it is important to bear in mind the three guarantees below, in order to check that the anonymization is correct:

- **Is it still possible to single out an individual?**
- **Is it still possible to link records relating to an individual? And;**
- **Can information be inferred concerning an individual?**

In conclusion, hashing technique implies storing hashes corresponding to each personal data in the blockchain network. Separately, personal data will remain stored in a database managed by a controller. In this way, modifying or removing personal data and therefore the exercise of data subject's rights according to GDPR is possible without perverting blockchain technology, i.e. keeping the immutability feature.

Blockchain Solution to GDPR Principles

Private channels: integration in blockchain

What are private channels?

Private channels are created in the blockchain network by two or more nodes that want to share information in a private way, i.e. nodes A and B don't want the rest of the nodes knowing which information (the content) they are sharing. The rest of the nodes (those who are out of the private channel) only will be able to know the hash of the corresponding information shared through the private channel.

The way of sharing information in a private channel: encryption

The data shared in the private channels should be encrypted. Encryption is a security practice which has the aim of providing the confidentiality of a communication channel between identified parties, avoiding eavesdropping or unintended disclosure. Encryption implies parties having a decryption key which allows to access to the information to everyone who receive said key, in this case, nodes A and B. The key is guarded by nodes A and B of the blockchain.

Why encrypted data?

Private channels are part of the blockchain and even though they are private, they have the same features as open channels within a blockchain, i.e. the personal data stored in them are immutable. The solution to this challenge is encryption of personal data.

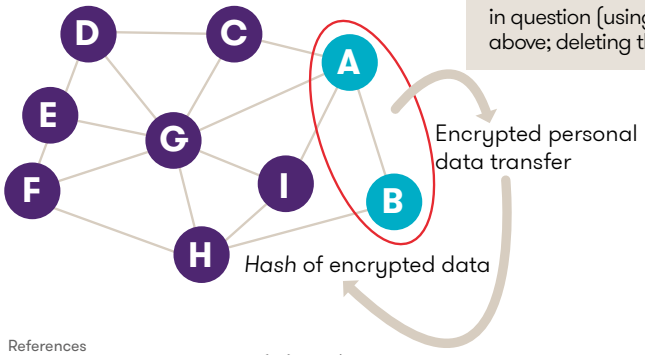
If personal data is encrypted, each time nodes A and B need to remove or update the information stored in the private channel according to GDPR principles, they would only need to remove the decryption key of the corresponding unit of personal data. The encrypted unit of data would remain in the private channel, but could not be visualized by either A or B.

Private channels with encrypted data: functioning

1 Nodes A and B create a private channel in the blockchain

2 Encrypted personal data are shared in the private channel between A and B

3 The hash of the encrypted data is stored in the "common" blockchain, i.e. the rest of the nodes (C, D, E, F, G, H, and I) know that A and B have shared information at a specific time but they are not able to see the content, they only see the hash.



How does this solution work?

Data removal: When the unit of personal data must be removed according to principles of lawfulness of processing or storage limitation, nodes A and B remove the decryption key of the corresponding encrypted personal data. This renders the data record unidentifiable and inaccessible (to all, including A and B), as the key in this case, has been deleted.

Data modification: In the event the data needs to be modified (according with accuracy principle), rather than modifying current data records, nodes A and B would effectively delete the record in question (using methods described above; deleting the decryption key).

The updated record would replace the former – where it receives a new encryption key. The previous record is now unidentifiable and inaccessible without the corresponding (deleted) decryption key.

Confidentiality: Since hashes are stored in the "common" blockchain and personal data remain stored in a private channel, the participants in the blockchain network (nodes C, D, E, F, G, H and I) would only have access to the hashes, random numbers with no perceived meaning, in isolation.

References
- European Parliament. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). April 2016.
- Article 29 Working Party. Opinion 05/2014 on anonymization Techniques, adopted on 10 April 2014. April 2014.
- Hogan Lovells. A guide to blockchain and data protection. September 2017.
- Guy Zyskind, Oz Nathan and Alex 'Sandy' Pentland. Privacy: Using Blockchain to Protect Personal Data.
- Chainfrog. Blockchain and GDPR, 2017.
- Pablo Fernández Burgueño. La obligación legal de cifrar información y datos personales. January 2017.

Conclusions

Compliance by Design

Using Blockchain, as any other innovative measure, needs a full legal assessment in order to address the possible challenges which may entail. Referred to as "compliance by design" it constitutes as a principle described in GDPR. This principle applied to Blockchain implies the need of designing it in such a way that makes it compatible with the law from the beginning.

Case by Case Solutions

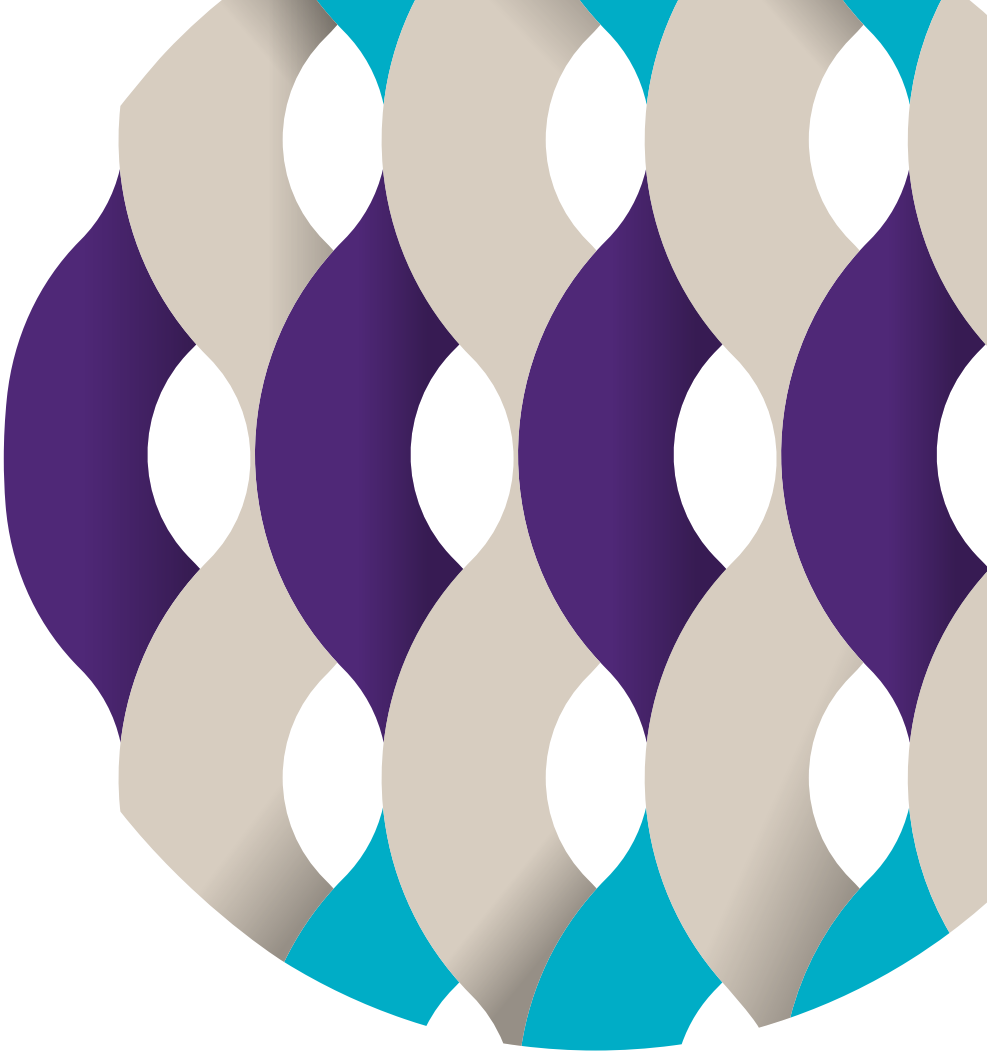
Protecting privacy in Blockchain is made possible by applying different methods; hashing, private channels, or a combination of both. These methods should be studied before designing a blockchain solution in order to determine which one fits better with the objectives of the initiative and the workflows of the entity in question - Particularly taking into account the importance of avoiding denaturing the main features of Blockchain technology.

Contacts

Luis Pastor
Head of Blockchain, Partner
+34 638 184 482
Luis.Pastor@es.gt.com

Adrian White
International Blockchain Initiatives
+34 659 639 467
Adrian.White@es.gt.com

Sara Esclapés Membrives
Professional Blockchain Lawyer
+34 676 644 691
sara.esclapes@es.gt.com



Grant Thornton

An instinct for growth™

grantthornton.es