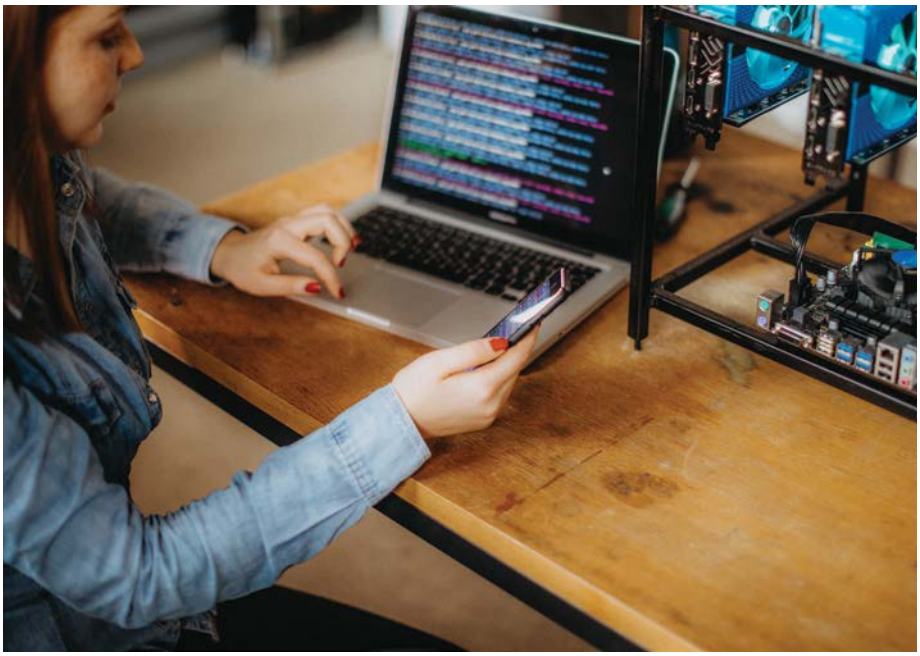
Blockchain: key challenges to get your solution GDPR-compliant



What is the General Data Protection Regulation (GDPR) about?

The **General Data Protection Regulation (GDPR)** (EU) 2016/679 harmonises personal data protection law on the territory of the European Union (EU). It stipulates rules on data processing and on the transfer of personal data in and outside the EU. Coming into effect on **25 May 2018,** it will replace the 1995 Data Protection Directive (Directive 95/46/EC). Non-compliance with the GDPR may lead under some circumstances to severe fines of up to 4% of worldwide annual turnover.

What are the key challenges the GDPR triggers for blockchain?

Depending on the blockchain-based activity the GDPR raises considerable legal concerns. Among the most relevant ones relate to the processing principles of data minimisation and storage limitation. Some key challenges relate specifically to blockchain features, such as:

1. Immutability of transactions

Transactions on a blockchain are immutable. It is not possible to delete information from a blockchain. This may contradict the GDPR's right to erase / duty to delete personal data when a lawful ground for processing ceases to exist. Throwing away the encryption keys may not be considered a valid means to comply with that duty.

2. Replication

Blockchain shares, as one of its key technical features, data across various nodes of a network. That raises issues not only with regard to erasure but also, and in particular, with regard to the principle of data minimisation. In other words, how much data spreading is necessary and how privacy by design and default applies with regard to blockchain.

Contacts

Dr. Guenther Dobrauz
Leader,
PwC Legal Switzerland, Zurich
+41 58 792 14 97
guenther.dobrauz@ch.pwc.com

Susanne Hofmann
Director,
PwC Legal Switzerland, Zurich
+ 41 58 792 17 12
susanne.hofmann@ch.pwc.com

Dr. Idir Laurent Khiar
Manager,
PwC Legal Switzerland, Zurich
+41 58 792 17 51
idir.laurent.khiar@ch.pwc.com

Orkan Sahin
Assistant Manager,
PwC Legal Switzerland, Zurich
+41 58 792 19 94
orkan.sahin@ch.pwc.com

pwc

3. Encryption

Encryption and hashing are fundamental to blockchain-based technologies. While both contribute to the principle of safeguarding the confidentiality and integrity of personal data in a blockchain, those means do not resolve the issue that hashed or encrypted personal data remain personal data under the GDPR and, thus, remain subject to its regulatory scope.

4. Data controllers and data processors

For data protection compliance purposes it is important to identify the roles of the different parties involved in various activities where data are processed. In a distributed ledger scenario a clear determination of the roles is challenging:

a. ***Data controllers***
A data controller determines the purposes and means of personal data processing.

b. ***Data processors***
A data processor processes personal data on behalf of the controller.

As a matter of fact, in a distributed ledger more than one party may qualify as controller for one category of processing (joint controllership) and may be responsible for compliance with the GDPR requirements. Further, as the applicable requirements depend on whether a party is a controller or processor for a certain processing activity, it is crucial to carefully assess the roles of the parties involved in a blockchain network. Specific agreements might be required among participants to define the responsibilities of each participant.

An aggravating factor is the circumstance that in many blockchain systems, no central operator or administrator exists, rather the system is operated by all its users in a peer-to-peer network environment. This means that every participant in the blockchain might be a data controller for himself, and a data processor for others (depending on the blockchain type).

			Read	Write	Commit	Example
Blockchain types	**Open**	*Public permissionless*	Open to anyone	Anyone	Anyone	Bitcoin, Ethereum
		Public permissioned	Open to anyone	Authorised participants	All or subset of authorised participants	Sovrin
	Closed	*Consortium*	Restricted to an authorised set of participants	Authorised participants	All or subset of authorised participants	Multiple banks operating a shared ledger
		Private permissioned ("enterprise")	Fully private or restricted to a limited set of authorised nodes	Network operator only	Network operator only	Internal bank ledger shared between parent company and subsidiaries

How PwC can support

We recommend to scrutinise your block-chain-based solution with regard to GDPR compliance to obtain a clear view of the legal risks you may encounter.