European Data Protection Board

May 2025

Use of blockchains

how to protect individual's personal data

A blockchain is a distributed digital database that keeps records across many computers and stores information about specific types of transactions. Many blockchains also support "smart contracts", which enable programmable transactions. For example, an insurance company might launch a smart contract technology to deal with flight delay insurance claims. The smart contract would be connected to global air traffic databases so that payment is automatically triggered if the flight experiences a specific delay.

One of the main advantages of blockchain technology is that it can offer strong availability and protection against data tampering thanks to cryptographic signature and hash functions as well as its decentralised nature. However, when blockchain is used to handle personal data, it also raises specific challenges regarding compliance with privacy laws like the GDPR.

The **EDPB guidelines on processing of personal data through blockchain technologies** help organisations to comply with the GDPR by analysing different blockchain architectures. The guidelines include 16 practical recommendations in its Annex A.

What are the different types of blockchains?

Blockchains can be grouped based on who can access them, who can participate in them, and who controls the system. There are usually two main characteristics of blockchains based on:

1 Whether the chain is open to everyone or not (public vs private)

2 Whether everyone can participate freely or not (permissionless vs. permissioned blockchains)

- **Permissionless blockchains:** in these blockchains, all computers (called "nodes") in the network have the same rights and capacities: they can join, read the data, add new information, or create new blocks (which are the building blocks of the blockchain that store transactions).
- **Permissioned blockchains:** in these systems, not all nodes have the same rights. What they can do depends also on the governance rules and who is in charge. Only approved participants - chosen by an authority running the blockchain, which can be a single entity or a group of entities - are allowed to join the blockchain and perform certain actions like reading data, adding new information, or creating new blocks.

Identify technical and organisational safeguards, and define roles early on

Organisations should **put in place appropriate technical and organisational measures** from the start. They should also **clearly define the roles and responsibilities of the different actors** as early as possible when **designing how the blockchain will process data.**

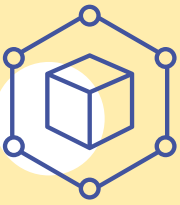
If the law does not already assign responsibilities, you should make a **factual assessment.** Elements to consider in this assessment may include the nature of the service provided, the governance of the blockchain, the technical and organisational features of the blockchain, and how the different actors are involved.

In addition, if you plan to use blockchains to handle personal data in a way that could pose a high risk to the rights and freedoms of individuals, you should also carry out a **Data Protection Impact Assessment (DPIA)** prior to the processing. This assessment will help you identify and mitigate the data-protection risks.

Assessing the risks to the rights and freedoms of individuals

Blockchain is just a technology, as cloud computing or peer-to-peer networks. It is not a processing of personal data as such. But **choosing to use blockchain technology can still affect how you handle personal data** and whether you are GDPR-compliant.

If you use blockchains, you should ensure that personal data is well protected and in particular that it is not accessible to everyone by default. **To assess the risks to the rights and freedoms of individuals**, ask yourself these key questions and document your answers:



1. Will any personal data be stored in the blockchain?
2. If yes, why is a blockchain the right tool for this (ie. is it necessary for this processing)?
3. What type of blockchain should be used (ie. public/private, permissioned/permissionless)?
4. What technical and organisational safeguards are in place?

Personal data on a blockchain?

1. Personal data in transaction metadata

Blockchains store metadata related to each transaction. This often includes user identifiers like public keys. If someone is using a personal public key, then it can probably be used to identify them, making it personal data under the law. The initial blockchains make this information visible to everyone. Some blockchains use advanced cryptographic tools, such as zero-knowledge proofs, to keep those identities hidden. These are usually called **"zero knowledge blockchains"**.

2. Personal data in transaction content

Transactions on a blockchain often include content, known as the "payload" of a transaction. This could be for example a cryptocurrency amount, a link to a document, an item purchased, or a smart contract action. Sometimes, this payload can also include personal data, either about the users involved in the transaction or other individuals.

Storing data off-chain

As a general rule, **you should avoid storing any additional personal data on the blockchain itself**, beyond the identifiers (or proof of identifiers in the case of "zero knowledge blockchains") needed to make the transaction. In this way, it is easier to respect privacy principles such as purpose limitation, data minimisation, accuracy, integrity and confidentiality.

Furthermore, **off-chain storage makes it easier to correct or delete data**.

A good approach is to store a cryptographic proof (like a hash or commitment) on the blockchain, but keep the actual personal data off-chain. This way, the blockchain can prove that data existed at a specific time, but it does not reveal the data itself. Once the off-chain data is deleted, the proof alone can't be used to identify anyone.

When on-chain storage of personal data is necessary

When you decide to store the payload on the blockchain, try to limit the data protection risks. Make sure that this decision is consistent with your purpose and data retention period. Evaluate the consequences of making those data public and decide on whether to store them on chain in clear or as encrypted text.

When data is no longer needed, you should delete or make it anonymous

You must **set a data retention period defining how long personal data should be kept**. When this period ends, you must **delete the data or anonymise it**. If you plan to keep the data for the entire lifetime of the blockchain, you should clearly identify why this is necessary, and document your reasoning.

Read the guidelines