TechGDPR

GDPR and Blockchain

Cheat Sheet

VERSION 1.2

01 What is the GDPR?

GDPR = the General Data Protection Regulation. It comes into effect on May 25th and requires companies to manage personal data in certain ways.

02 Does it apply to my company?

Probably. The regulations apply to every company, anywhere in the world, that deals with data of subjects that are in the EU, or when targeting Europeans.

03 What if I do nothing?

You can get fined and the fines are larger than before. Fines go up to € 20M or 4% of annual group turnover, whichever is higher.

04 What is personal data?

Personal data by the definition of the GDPR is any information relating to an identified or identifiable natural person.

05 How does this apply to blockchains?

In general, it is advised to stay away from storing personal data on a blockchain because there are some potentially significant incompatibilities, like immutability: the GDPR ensures that data subjects under certain circumstances have the right to have their data corrected or deleted which is impossible on an immutable ledger.

06 Can I store unlinked or hashed data to avoid it being considered personal data?

This is unclear and compliance is untested. It is unknown where to draw the line with identifiable data when used in blockchains. However, you can research similar non-blockchain efforts and past data protection regulations to get an idea in specific circumstances.

07 Pseudonymised and Anonymised Data

Pseudonymised personal data can be linked to a natural person by using additional information, and is considered a security mechanism under the GDPR, but is still in-scope personal data. Anonymised personal data is the data that is completely anonymous and can never be related back to a person, and therefor out of scope of the GDPR. It has to be assumed that for example a wallet address is considered pseudonymised data, as it can be led back to a natural person through KYC information collected by an exchange or ICO.

08 Who is a data controller?

A data controller is a party that determines the purposes and means of the processing of the personal data.

09 Who is a data processor?

A data processor is a party that receive the data and are only supposed to process it on behalf of the controller, and only with a legal contract in place.

10 Who is the controller and processor with blockchains?

Where there is no party in control or many parties in control like in public blockchain environments, it is unclear how these roles will be applied. It should be assumed that any central entity such as company or foundation that is controlling or has developed the network will be held liable until this can be proven not to hold up under case law.

11 What about private & permissioned ledgers?

Even though there is a higher level of control in permissioned and private blockchains, and the controller and processor positions are much clearer, it is still not easily possible to comply with all the Subject Access Rights.

12 What about KYC / AML information?

When you are collecting KYC / AML information for an ICO, or as an exchange, this may even contain special categories of personal data that requires additional protection and a due process to evaluate how data is stored and secured.

So, What Should I do?

Analyze why you are collecting personal data to begin with:

A legal base for processing of personal data is always required. This could for example be the performance of a contract, a legitimate interest, compliance with a legal obligation or the consent given by the subject involved. It will always need to be specific for the purpose of the processing and transparent about how the data is stored and used.

Determine internal processes to handle personal data:

Subjects of whom you are storing personal data have their access rights, based on which they can request you to tell them what information you are storing on them, and request to delete, block or correct it. Be ready to deal with these within 30 days!

Don't store unnecessary personal data:

Data should not be stored any longer than required for the purpose you are storing / processing it for. If you are changing the purpose of storing or processing the data, you will need a new legal ground, and in case of consent, renewed, specific consent.

Document what compliance efforts you are taking:

The GDPR requires you to build up documentation about your compliance efforts. While is is nearly impossible to comply for 100% with the regulation, it is crucial to demonstrate what has been done to protect the interests of data subjects and to document your processes, requests, breaches and persons involved.

TechGDPR can help with your compliance process, in particular for Blockchain, AI, IoT and Cloud technologies. Contact us for a free chat about the impact of the GDPR for your company on **contact@techgdpr.com**.