**What is GDPR?**

*“The improvement in substance is that there’s far more transparency under the new rules, which means that you will have more detailed information policies about what your data are processed for, which purposes if they are given to others, and there will be also in general more possibilities to get a view of which data are there about you. And you have new rights like data portability and the right to be forgotten. So, it will be far easier for consumers to control their personal data.”*

- Jan Philipp Albrecht, member of the European Parliament and ‘father’ of the GDPR (3)

The General Data Protection Regulation (GDPR) was created from the European Commission to reform data protection across the European Union in order to make Europe ‘fit for the digital age’. (1) The origins of what is now known as the GDPR began in 2012. All organizations in the member-states across Europe, including those who have dealings with businesses in Europe must adhere to the GDPR EU framework. The GDPR was approved and adopted in April 2016 but was not enforced until May 25, 2018. (2)

“The key changes in the reform include:

* A **single set of rules** on data protection, valid across the EU. Unnecessary **administrative requirements,** such as notification requirements for companies, will be removed. This will save businesses around €2.3 billion a year.
* Instead of the current obligation of all companies to notify all data protection activities to data protection supervisors – a requirement that has led to unnecessary paperwork and costs businesses €130 million per year, the Regulation provides for increased **responsibility and accountability** for those processing personal data.
* For example, companies and organisations must notify the national supervisory authority of serious **data breaches** as soon as possible (if feasible within 24 hours).
* Organisations will only have to deal with a **single national data protection authority** in the EU country where they have their main establishment. Likewise, people can refer to the**data protection authority** in their country, even when their data is processed by a company based outside the EU. Wherever **consent** is required for data to be processed, it is clarified that it has to be given explicitly, rather than assumed.
* People will have easier **access to their own data** and be able to **transfer personal data** from one service provider to another more easily (right to data portability). This will improve competition among services.
* A **‘right to be forgotten’** will help people better manage data protection risks online: people will be able to delete their data if there are no legitimate grounds for retaining it.
* EU rules must apply if personal data is **handled abroad**by companies that are active in the EU market and offer their services to EU citizens.
* **Independent national data protection authorities** will be strengthened so they can better enforce the EU rules at home. They will be empowered to fine companies that violate EU data protection rules. This can lead to penalties of up to €1 million or up to 2% of the global annual turnover of a company.
* A new**Directive**will apply general data protection principles and rulesfor **police and judicial cooperation** in criminal matters. The rules will apply to both domestic and cross-border transfers of data.” (1)

The GDPR at its core is powerful and needed, however, the application of it interferes with the premise behind Blockchain Technology. In 2012 when the European Commission first introduced the GDPR, blockchain was not a known word and the GDPR idea was initially focused on cloud services and social networks.

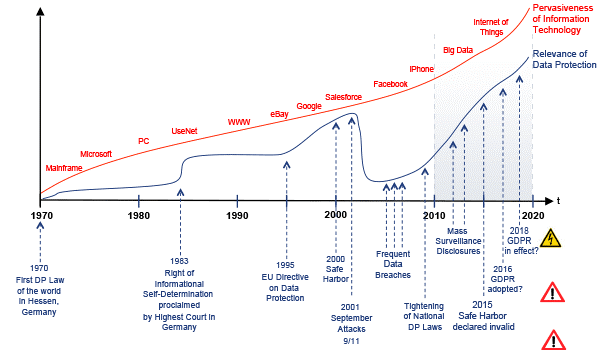


Figure : A brief history of the General Data Protection Regulation by Wilhelm (2016) (4)

**Implications of GDPR for Blockchain**

The table below, summarized from The Journal of The British Blockchain Association, summarizes the implications related to blockchain and GDPR. (3)

|  |  |  |
| --- | --- | --- |
| **GDPR Article/Recital** | **Implications** | **Topic** |
| Art. 4(1), 6(4), 32/Rec. 26 | Can PD be stored on a blockchain or must be off-chain? The connection between pseudonymized and anonymized data and the data subject. | **Personal data on the blockchain** |
| Art. 6 | Six reasons can be used to comply with lawful processing, and a data sharing agreement can be recorded on a BC | **Lawful Processing in the EU/Consent** |
| Art. 17, 17(1), (a,b), 6(1)(b,f)/Rec. 69 | Can data on a blockchain be deleted in accordance  to the RTBF and what would happen if not – could  the functioning principle take over that allows for  specific interpretations of the GDPR, as BC is at its  core designed not to be compliant to the RTBF. | **Right to be forgotten (RTBF) and functioning principle** |
| Art. 25/Rec. 78 | BC runs counter to data minimization, storage limitations and a clearly determined data controller, raising the question whether it is in line with ‘Privacy by Design’ (PbD). Privacy risks of entire IT-architecture, including BC. Solutions could be Enigma or differential privacy or future more secure BCs. | **Privacy by Design versus blockchain core features** |
| Art. 26(1)/Rec. 79 | Private versus public BC and the accountability of a (joint) data controller. | **Accountability of data controller** |

**Article 4**

Article 4 of the GDPR defines personal data. The definition is very broad which complicates it’s interpretation with the use of blockchain. (7)

**Article 6**

Article 6 discusses the consent that must be given. Such consent must have already undergone a thorough academic and practical discourse. (5) This means that consent must be “freely given, specific, informed and unambiguous”.

**Article 17**

Article 17 of the GDPR grants EU citizens the ‘right to be forgotten and to data erasure’ at any time upon request. Due to the immutable nature of blockchain, this presents a challenge. This is probably the largest challenge of GDPR and Blockchain.

**Article 25**

Article 25 of the GDPR discusses handling personal data by the concept of Privacy by Design. Privacy by design is privacy such that it “should be promoted as a default setting of every new IT system and should be built into systems from the design stage” (6). The blockchain implication is that the data must not be stored in plaintext. GDPR does not provide many details to this and has left it up to some interpretation. (5)

**Article 26**

Article 26 discusses the description of who is responsible. This must be completed in a transparent manner in order to be in compliance, which can be a challenge when there are joint data controllers.

1. <http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en>
2. <https://www.trunomi.com/eu-gdpr-compliance-trunomi/>
3. <https://jbba.scholasticahq.com/article/3554.pdf>
4. “A brief history of the General Data Protection Regulation.” <https://iapp.org/resources/article/a-brief-history-of-the-general-data-protection-regulation/>
5. <https://dl.eusset.eu/bitstream/20.500.12015/3159/1/blockchain2018_03.pdf>
6. Bert-Jaap Koops and Ronald Leenes. 2014. Privacy Regulation Cannot Be Hardcoded. A Critical Comment on the ‘Privacy by Design’ Provision in Data-protection Law. Int. Rev. Law Comput. Technol. 28, 2 (May 2014), 159–171.
7. <https://www.blockchainandthelaw.com/2018/04/blockchain-personal-data-and-the-gdpr-right-to-be-forgotten/> (I know this isn’t a journal…I’ll try to find something ‘better’ before final submission)

***##Find and Discuss specific GDPR articles that related to blockchain. Unpack each one with a few sentences or small paragraph.***

***## Potential sources (not journals – just gathering info to read)***

* [***https://cointelegraph.com/news/gdpr-and-blockchain-is-the-new-eu-data-protection-regulation-a-threat-or-an-incentive***](https://cointelegraph.com/news/gdpr-and-blockchain-is-the-new-eu-data-protection-regulation-a-threat-or-an-incentive)
* [***https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data***](https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data)
  + [***https://www.insideprivacy.com/financial-institutions/the-cnil-publishes-report-on-blockchain-and-the-gdpr/***](https://www.insideprivacy.com/financial-institutions/the-cnil-publishes-report-on-blockchain-and-the-gdpr/)
* [***https://www2.deloitte.com/dl/en/pages/legal/articles/blockchain-datenschutzrecht.html***](https://www2.deloitte.com/dl/en/pages/legal/articles/blockchain-datenschutzrecht.html)
* [***https://www.hlengage.com/\_uploads/downloads/5425GuidetoblockchainV9FORWEB.pdf***](https://www.hlengage.com/_uploads/downloads/5425GuidetoblockchainV9FORWEB.pdf)
* [***https://medium.com/varanida/gdpr-results-impacts-and-the-blockchain-opportunity-d9f368d347aa***](https://medium.com/varanida/gdpr-results-impacts-and-the-blockchain-opportunity-d9f368d347aa)
* [***https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules\_en***](https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en)