EU Blockchain Observatory and Forum Workshop on GDPR, data policy and compliance

(08.06.2018, Brussels) : Report

Ferrari, V.; Quintais, J.P.; Giannopoulou, A.; Bodó, B.

Publication date
2018

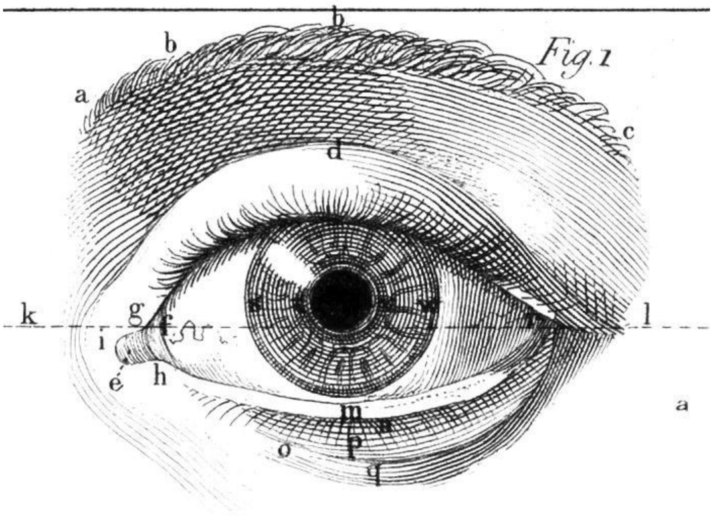
Document Version
Final published version

License
CC BY-NC-ND

Link to publication

Citation for published version (APA):
Ferrari, V., Quintais, J. P., Giannopoulou, A., & Bodó, B. (2018). *EU Blockchain Observatory and Forum Workshop on GDPR, data policy and compliance: (08.06.2018, Brussels) : Report* . (Blockchain & Society Policy Research Lab Research Nodes; No. 2018/1). University of Amsterdam, Institute for Information Law. https://blockchain-society.science/wp-content/uploads/2018/07/blockchain_society_research_nodes_1_GDPR_workshop_03072018.pdf

EU Blockchain Observatory and Forum
Workshop on GDPR, data policy and compliance
(08.06.2018, Brussels)
Report



University of Amsterdam

Institute for Information Law

Blockchain & Society Policy Research Lab

Research Nodes 2018/1

V. Ferrari*, PhD candidate
with contribution from J.P .Quintais*, A. Giannopoulou*, B. Bodo*
*Blockchain & Society Policy Research Lab, Institute for Information Law (IViR), University of Amsterdam (UvA)

***

The EU Blockchain Observatory and Forum (an initiative led by DG CONNECT) organized the “Workshop on GDPR, data policy and compliance” event in June 2018 to discuss data protection issues as well as privacy-enhancing features of blockchain technologies. The meeting gathered stakeholders and experts to examine the main challenges and opportunities of distributed ledger technologies (DLTs), so supporting the European Commission’s efforts to provide practical guidelines for the industry.

Ms. Valeria Ferrari, of the Blockchain & Society Policy Research Lab participated in the workshop, and compiled this report.

Highlights

- The General Data Protection Regulation (GDPR) is tailored to the model of centralised storage of data. However, data stored on blockchains does not fall outside its application.
- For the storage of data, blockchains primarily rely on hashing and encryption techniques. These, however, do not necessarily entail data anonymity but only pseudonymity. As such, the storage of personal data on blockchain triggers the application of the GDPR, thereby increasing the risk of violations.
- Some GDPR requirements and principles are in strong tension with the structure of blockchain technology: e.g. the right to erasure, the principle of data minimisation and the conditions for transmission of data to third countries seem not to be applicable, unless interpreted in a tailored manner;
- At the state of the art, the only suitable approach to ascribe liability under the GDPR is a case-by-case assessment of parties' roles and activities;
- Technological solutions are under development, but they rely on cryptography which might be insecure in the long run.

Introduction(s)

The morning session was opened by Olivier Micol (DG Just, Head of Unit) with an introduction about the fundamental principles and rules of the EU General Data Protection Regulation (GDPR). The instrument – which is the result of a long negotiation among stakeholders and institutions – came into force on 25 May 2018. Before examining the interactions between blockchain and data protection within the EU legal framework, it is crucial to elucidate the key concepts and principles set out in the GDPR.

A first clarification that is important for the discussion is that – due to the ECJ's broad interpretation of "personal data" – pseudonymous data are covered by the GDPR, while only anonymous data fall outside its scope. Therefore, to avoid possible violations, businesses should refer to privacy authorities as to what is considered a valid anonymization technique.

Central to the GDPR are the concepts of accountability and controllership. The data controller (or the joint controllers) has(ve) duties to safeguard the respect of data subjects' rights. The legal instrument specifies six conditions under which data processing is legitimate[1]; the absence of at least one of these conditions makes the processing illicit. Another important principle is that of data minimisation: the purpose of the processing must be specified from its beginning, and the data should be deleted when no more required for the specified purpose. The data must also be accurate and correct: if necessary, data subjects are now granted tools to request its amendment. Moreover, specific rules are provided for the transfer of data to third countries.[2]

Crucial for the effectiveness of the GDPR is the possibility for individuals to enforce the rights provided therein. To this aim, in each country a Data Protection Authority (DPA) is established. This is an independent authority in charge of enforcing the GDPR rules, without prejudice to any rights

[1] According to Article 6 of the GDPR , "Lawfulness of processing", the processing of data is lawful if at least one of the following conditions are met: consent for the processing has been given from the data subject; the processing is necessary for the performance of a contract to which the data subject is party; the processing is necessary for compliance with a legal obligation; the processing is necessary to protect "vital interests" of a natural person; the processing is required by reasons of public interest or for the exercise of official authority; the processing serves the pursuit of legitimate interests.

[2] Rules are contained in Chapter 5, GDPR, "Transfers of personal data to third countries or international organisations".

or remedies to which individuals may be entitled in their national jurisdiction. In addition, to ensure a harmonic interpretation and application of the GDPR, the European Data Protection Board acts as central interlocutor for the DPAs.

1. Blockchain and GDPR (Michèle Finck)

After the brief but essential overview of the GDPR core rules and principles, Michèle Finck took the stage to highlight the major points of tension between the European legal instrument on data protection and blockchain technology.

The GDPR, she noted, has a twofold objective: to ensure free movement of personal data within the EU; and to protect fundamental rights, conferring on data subjects more control over personal data. In pursuing these goals, the instrument, drafted more than two years ago, assumes that the data is stored and processed in centralized databases. On the contrary, Blockchain technology – at least in its permissionless version – is a system for decentralized collection, storage and processing of data. Given its peculiar architecture, several provisions of the GDPR fall short when applied in this context.

A first question to be addressed is whether the GDPR is at all applicable when data is stored on distributed ledger technologies with no central party having exclusive control over it. The answer, according to Michèle Finck, is simple: GDPR applies whenever personal data is at stake, unless it is anonymized.[3] As on blockchains data is generally not anonymous but only pseudonymous, the GDPR applies.

Data stored on blockchains can be classified in two main categories: (i) transactional data, such as messages and transactions of various kinds occurring among users; and (ii) public keys: users' personal identifiers. The latter unquestionably qualify as personal data.

Another important distinction regards the form in which data can be stored on blockchains, namely as plain text, encrypted or hashed. The former clearly does not prevent potential GDPR violations if personal data is concerned; and, anyway, it is costly, inefficient, and therefore very unusual. Furthermore, the higher degree of confidentiality ensured by encryption and hashing does not represent a safe harbor from data protection liability. Given that encrypted data may always be reversed and hashes can be linked to the data they have been derived from, these techniques do not guarantee anonymity but merely pseudonymity. Consequently, encrypted or hashed personal data stored on a blockchain fall within the scope of the GDPR.

After clarifying the applicability of the legal instrument, Michèle Finck proceeds by stressing out the shortcomings of the GDPR when applied in a blockchain context:

- The complexity of identifying the data controller, especially at the protocol layer (easier at the application layer);
- The impracticality of complying with the prohibition of processing data in third countries, where no equivalent protections are in place;
- The uncertainty about the factual application of the principle of data minimization;
- The enforceability of the right to amend and (of) erasure of personal data in tamperproof blockchains;
- The enforceability of the protection against automated processing of personal data.

The analysis of GDPR requirements and blockchain technical features leads to pessimistic and optimistic conclusions. The former are based on the acknowledgment of the apparently irresolvable

[3] Meaning that the identification of the subject they refer to is irreversibly prevented.

incompatibilities between data protection rules and blockchain. First and foremost, in a blockchain scenario, we lack tools to identify the subject of GDPR obligations and, consequently, to enforce data subjects' rights. Confusion comes from the terminological uncertainty around the concept of "erasure", a GDPR requirement which seems to be problematic for the inherent immutability of blockchains. Moreover, it is unclear whether hashing – the most common method used to achieve confidentiality of blockchain data – could ever be considered an anonymization technique. On top of this, it must be noted that most blockchain-based projects are, so far, not compliant with GDPR requirements. Therefore, it is legitimate to question, on one hand, whether DLTs could threaten data protection in the EU and, on the other, if the current legal uncertainty about the application of the GDPR could hinder innovation.

The optimistic conclusions relate to the concept of "data sovereign" as a shared objective of both blockchain-based projects and communities. Notwithstanding the current technical obstacles to data protection, the technology is still immature and could be further developed to better fit privacy requirements. In the future, there could and should be a greater techno-legal interoperability: blockchain could be deployed to ensure data protection by design and to combine privacy with transparency. Indeed, what is needed is a strong cooperation between stakeholders for the further development of the technology and for a proper, tailored interpretation of the GDPR.

2. BCDiploma (Alexis Berolatti)

The second speaker, Alexis Berolatti, presented its project "BCDiploma": an application that "dematerializes" the issuance of school diplomas ensuring authenticity of data and confidentiality of information through blockchain technology. With a simple click, users can display their degrees' attestation. The platform ensures the reliability of the certification and of the issuer thereof. All information is, in fact, previously verified by the company and embedded in the Ethereum public blockchain; when needed, the student can exhibit their education records without revealing additional, unnecessary information.

The concerned data are the name of the student, date and place of birth, degrees, and other personal information. Hence, the solution requires personal data processing activities, regulated by the GDPR. Under this legal instrument, the legal basis for the processing is the students' consent, whereas the objective is to allow students to share their certified data with third parties. The party responsible for the data processing is not the company providing the platform, but the diploma issuer (i.e. the school).

The solution ensures compliance with the GDPR as it deploys a safe encryption algorithm and a 3-keys assembly which ensures high standard security and possibility of erasure. It is, in fact, possible to make data unreadable by deleting one of the three keys. Moreover, the application impedes data exploitation and provides access and dissemination control.

Notwithstanding the pragmatic and innovative approach of the BCDiploma solution, the storage of personal data on the blockchain – even if hashed or encrypted – keeps raising some concerns. For instance, if the encryption ever gets broken, the data would remain immutable and publicly accessible on the Ethereum blockchain, certainly causing violations of data protection rights.

3. Panel discussion (Michèle Finck, Elizabeth Reniers, Jörn Erbguth, Alexis Berolatti)

The panel discussion was kick-started by Elisabeth Reniers, who introduced the issue of the allocation of liabilities for GDPR compliance in a blockchain environment. The primary problem, as already mentioned by Michèle Finck, is that of identifying the data controller and data processors. Here, the tension between the structure imagined by the GDPR and the decentralized, self-sovereign architecture of blockchain technology becomes clear.

Three rules should govern the allocation of liability in this context: (i) to look at the factual activities, not at the formal position of a party; (ii) to focus on allocation of responsibilities; (iii) to explain with sufficient clarity how the law should be effectively applied.

As it regards the implementation of the data self-sovereign model, Elisabeth Reniers pointed to the need to consider making data subjects the data controller. The GDPR would not prevent this approach, but it would be necessary to provide interpretations of the regulation that fit this situation.

The panel discussion turned then to the definition of personal data. Similarly to IP address, hashes and private keys are generally considered to be personal data. However, it is always necessary to look at the actual case, considering, for instance, who stores and has access to the private keys and the likelihood that the encryption will be broken within a given period of time.

One argument raised during the discussion was that encryption could always, at some point in time, be broken. However, it was noted that this is not a peculiarity only found in hashing techniques. Data considered to be properly anonymized could be reversed to its original. Therefore, what makes blockchain storage more problematic than traditional methods of recording data is its potentially unlimited duration.

The decentralized nature of the technology and, consequently, of the data processing extends to any service provider and even to any user running a blockchain node potential liable under Article 29 of the GDPR[4]. Therefore, to counterbalance the wide scope of application of the GDPR in a blockchain-based context, more tailored interpretations on whether private keys and hashed data qualify as personal data should be provided in future case law.

The protection from automated decision-making as set out in Article 22 of the GDPR, mentioned by the panelists, does not raise special issues in the context of blockchain scenarios. The article, in fact, tackles the use of Artificial Intelligence (AI) to automate transactions; blockchain-based automation of transactions (so called "smart contacts") generally provides greater auditability and transparency compared to other methods of executing algorithmic-based transactions.

One of the GDPR requirements that may be more problematic to implement in blockchain environments is that of ensuring the right to data erasure (Article 17). However, there is no univocal interpretation of what "erasure" means in practice; therefore, a risk-based, case-by-case assessment will be necessary for a correct application of the regulation.

Ultimately, Article 3 sets out a broad geographical application of the GDPR. Given the difficulty of geographically limiting blockchain-based networks, a global approach to data protection would, in this context, be necessary.

The various issues that emerged from the discussion suggested that technological, governance, and legal solutions must be simultaneously thought out in order to tackle the possible clash between blockchain adoption and GDPR compliance.

[4] "Processing under the authority of the controller or processor".

On a technological level, the most common solution for scalability as well as privacy problems in blockchains is "hashing out", i.e. pushing as much data off the ledger as possible. Only transactional data should be recorded on blockchains, while any credential or identifying information should be stored locally with the end user. This approach characterizes "zero-knowledge proof" kinds of solutions, which effectively lower the risk of liability for GDPR violations.

Besides strategies which imply minimal share of data, blockchain is interesting from a privacy perspective as it provides auditability, transparency and data portability. Opening access to data creates unique economic opportunities and blockchain offers the possibility to overcome current models where data are captured into silos.

The panelists pointed out that, when discussing privacy issues, the governance of a given technology is decisive for the attribution of responsibilities. In a blockchain scenario, for instance, a majority of nodes having control over the network could be identified as a data controller. In this context, not only on-chain governance but also off-chain dynamics and activities deserve full attention (i.e. oracle functions, etc.).

Finally, as to the legal responses, the stakeholders seem to agree that a principle-based, industry-driven (rather than technology-driven) approach is preferable for the establishment of code of conducts or legal guidelines for the blockchain ecosystem. The goal of legal guidelines should not be to curb innovation but to support the development of the industry within a clear regulatory framework. For this reason, self-regulation is more suitable than top-down regulation, the latter being in total contradiction with the horizontal, decentralized paradigm of blockchain. Nonetheless, it is law that should influence the technology, and not the other way around.

4. Workshop

The afternoon session, introduced by Claire Bury, Deputy Director General at DG CONNECT, was dedicated to an open discussion between the invited speakers and the participants of the working group.

Topics proposed for the discussion are the following:

- How compliance with GDPR could be achieved within the current framework?
- What are the challenges met by companies trying to build GDPR compliant solutions based on blockchain?
- How Blockchain could enable data protection and privacy by design?

4.1 Technical solutions

At a technical level, there is consensus on the fact that personal data should not be stored on the ledger. Moreover, feasible technical solutions that lower the risk of GDPR violations are available, such as address obfuscation, non-reversible transformation of personal information, offline storage of data and homomorphic encryption.

However, entrepreneurs (including startups, open-source projects, large companies' platforms) are concerned about some technical issues that should be clarified, namely:

- Is it prohibited to share with third parties encrypted (reversible transformation) data, unless the decryption of that data after a given time would not be relevant?
- Are there obfuscation methods which could prevent GDPR applicability?
- Are there data transformation methods which could prevent GDPR applicability?

4.2 Governance solutions

Assessing responsibilities under data protection law requires the deployment of a case-by-case approach; one that looks at roles and functions of the actors dealing with the data and at the reasons for the processing thereof.

When blockchain is the underlying technology for data exchange or storage, two main scenarios should be considered: (i) a user using a platform that processes data with a blockchain as a backend; and (ii) a user sending transactions directly through the blockchain or via a transformation service. In the first case, the question is whether the same frameworks applied to traditional web services could be valid in this context, with the consequence of considering, for instance, application-providers as data controller and wallet-providers, nodes and other service-providers as processors. The latter scenario, instead, raises the issue of whether end-users could qualify as data controller and, in that case, which actors should be considered data processors. As noted, there is no single solution for a type of scenario. Rather, each situation requires an assessment of the actual dynamics at play.

4.3 Legal solutions

The legal solutions were discussed through a case study concerned with the right to erasure. The extract of an open source development platform's Terms of Service and Privacy Policy was presented as an example of an original solution to blockchain and GDPR incompatibilities. In this example, the acceptance by the user of the Terms of Services and Privacy Policy would also result in the user knowingly waiving his right to request data erasure, removal or rectification. In this context, the relevant document stated that the user "[...]*understand*(s) *the removal of this information would be impermissibly destructive to the project and the interests of all those who contribute, utilize, and benefit from it. Therefore, [...]* (he) *waive*(s) *any right to request any erasure, removal, or rectification of this information under any applicable privacy or other law* [...]".

This case leads to some open questions. First, in which situations, if any, can the right to erasure be waived? Indeed, there are cases where the right to erasure does not apply, for instance when keeping records of transactions is required for Know Your Customer (KYC) and Anti-Money Laundering (AML) compliance. Moreover, what are the best practices when it comes to consent and Terms of Service? What steps and procedures are necessary to determine if a business is compliant with the GDPR? To be aware of potential violations, the GDPR imposes on companies an obligation to conduct "data protection impact assessments", aimed at identifying and mitigating privacy risks with data processing activities. However, specific codes of conduct may be beneficial for a correct development of blockchain-based applications and businesses.

5. Conclusions

The final "wrap-up" summarized points of consensus resulting from the working session and the main questions left unsolved. There was agreement on the fact that, in most cases, putting personal data on a blockchain is neither advisable nor necessary. As to assessing potential data protection liabilities in a blockchain scenario (e.g. identifying who qualifies as data controller and data processor), it is necessary to deploy a case-by-case approach, looking at facts and technical elements, like the type of blockchain at issue and the justification for processing data.

To mitigate the risk of GDPR violations, companies could resort to obfuscation and data transformation methods, such as ring signatures, zero knowledge proofs and peppered hashes. While these methods are currently considered robust, they rely on encryption that could be broken at some point in time. As a result, their suitability for privacy protection could be based on the expected time length of effectiveness. Finally, despite the serious concerns blockchains raise in relation to data protection, projects like Sovrin, Evernym and Decode were identified as examples of how this technology could successfully be implemented to improve privacy and data sovereignty.

However, some questions remain unsolved and their resolution will require greater techno-legal cooperation. from a technical standpoint, businesses must be assured if technical solutions like peppered hashes fall or not within the scope of the GDPR. Additional clarity is also needed for other obfuscation and data transformation methods: what are valid tools to prevent GDPR violations? For how long do they need to be proved resistant (e.g. until the data becomes irrelevant)?

To offer businesses some direction on how to tackle the challenges at the intersection of blockchain and GDPR, the EU Blockchain Observatory and Forum will foster the adoption of guidelines aimed at resolving these and other emerging uncertainties.

REFERENCES:

Finck, Michèle, Blockchains and Data Protection in the European Union (November 30, 2017). Max Planck Institute for Innovation & Competition Research Paper No. 18-01. Available at SSRN: https://ssrn.com/abstract=3080322 or http://dx.doi.org/10.2139/ssrn.3080322

Finck, Michèle, Blockchain Regulation (August 7, 2017). German Law Journal, 2018, Forthcoming; Max Planck Institute for Innovation & Competition Research Paper No. 17-13 . Available at SSRN: https://ssrn.com/abstract=3014641 or http://dx.doi.org/10.2139/ssrn.3014641

Halpin, Harry, Piekarska, Marta, Introduction to Security and Privacy on the Blockchain, 2017 IEEE European Symposium on Security and Privacy Workshops, April, 2017, Paris, France, available at: https://www.researchgate.net/publication/318126114_Introduction_to_Security_and_Privacy_on_the_Blockchain.

Ibáñez, Luis-Daniel, O'Hara, Kieron, Simperl, Elena, On Blockchains and the General Data Protection Regulation, June 3, 2018, University of Southampton.

The Lab has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme under grant agreement No 759681.