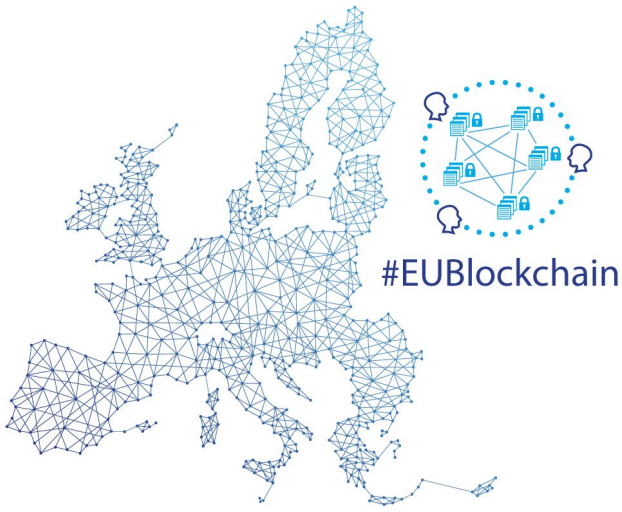
EU Blockchain Observatory and Forum

An initiative of the European Commission

EU BLOCKCHAIN OBSERVATORY AND FORUM

Workshop Report - GDPR

Brussels, June 8, 2018



By the European Commission, Directorate-General of Communications Networks, Content & Technology.

Author: Tom Lyons

Published on July 23, 2018

Comments and inquiries may be addressed to the following email: info@eublockchainforum.eu

Table of Contents

Context

The General Data Protection Regulation, which came into application in the EU on May 25 2018, is one of the most sweeping pieces of data protection and dissemination legislation in Europe in a generation.

On June 8, the EU Blockchain Observatory and Forum held a workshop to examine the clashes and correlations between blockchain technology and GDPR, and to provide as far as possible some guidance to technologists, lawyers, entrepreneurs and citizens looking to understand the implications of GDPR on the nascent blockchain industry.

Below are some of the highlights of the presentations and discussion:

Introduction to the day - DG CONNECT - Observatory & Forum / Pierre Marro & Chiara Mazzone

- GDPR is a very important issue for the EU.
- We are making use of personal data in an unprecedented way and unprecedented scale.
- Data is a fundamental right. GDPR explicitly says natural persons should be able to have control of their personal data.
- So the question for the workshop is: how can decentralized technologies provide solutions for this?

Introduction – Olivier Micol, Head of Unit, DG JUST – European Commission

- The right to the protection of personal data is a fundamental right, enshrined in the EU Charter of Fundamental Rights
- The GDPR, wants to give control to data subjects, and there is convergence with the spirit of blockchain on this points.
- The GDPR, adopted after a long negotiating process, provides the regulatory framework for the years to come.
    - One of the political goals of the GDPR is to give data subjects more control over their data; thus, there is convergence with the spirit of blockchain on this point.
- Key concepts in GDPR relevant to blockchain include:
    - **Personal data:** Personal data is any information relating to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly. To determine whether a person is identifiable, account

should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person. The CJEU has traditionally taken a broad interpretation of what constitutes personal data. Only anonymous data falls out of the scope of the GDPR (i.e. data that have been irreversibly anonymised). In this light, Article 29 WP, in Opinion 05/2014 on Anonymisation Techniques provides guidance. Pseudonymised data are personal data.

- **Controllership:** the identification of a controller and/or joint controllers is required and the GDPR emphasises the principle of accountability of the data controller. The controller needs to implement appropriate technical and organisational measures to ensure and be able to demonstrate compliance with the GDPR. In the case of joint-controllership, they need to, in a transparent manner, determine their respective responsibilities, in particular as regards the exercising of data subject rights; in case of joint controllership, the data subject can exercise his rights against any of the joint controllers (right of access, portability, rectification, erasure, etc.).

- **Data protection by design:** The controller is obliged to implement the data protection principles and ensure that any tool, service or product used for the processing has to be designed to take data protection into account intrinsically and right from the start (not as a layer on top).

- **Principles of data protection:** the GDPR is merely an evolution and not a revolution: It builds on the data protection concepts and principles in place in the EU for the last 20 years (such as purpose limitation, data minimisation, storage limitation), adding the principle of transparency and the principle of integrity and confidentiality.

- Grounds for processing: When processing data the first thing to do is to identify on what legal basis the processing can take place. There are six (6) bases: consent, performance of a contract, vital interest of the data subject, legitimate interest of controller, legal obligation, public interest.
  - In case personal data is transferred to a third country (i.e., outside of the EU) the rules regulating international transfers have to be respected.
  - The GDPR ensures that data subjects can have their rights enforced effectively. Each Member State has to set up a data protection authority whose tasks are to monitor and enforce the application of the law. Amongst its powers, a data protection authority may levy fines up to 4% of global turnover or 20 million euros. The GDPR sets up also the EU Data Protection Board (previously the Article 29 Working Party), which regroups the 28 national data protection authorities. The EDPB ensures consistency of enforcement. The GDPR introduces a one-stop-shop mechanism to ensure a uniform and consistent

application in all Member States. In case data protection authorities disagree on cross-border cases, the EDPB will be called on to issue binding decisions. This will ensure the uniform application of EU rules and prevent the same case being dealt with differently in different Member States.

- The GDPR offered Member states the flexibility on whether and to what extent administrative fines could be imposed on public authorities. Some have said yes, some have not. As with all regulators and enforcers, decisions of the national data protection authorities and the EDPB can be contested in the courts.

Presentation - Michèle Finck: Blockchain and GDPR

- People tend to forget that GDPR has a dual objective: fundamental rights protection, but also facilitation of the free movement of personal data in the EU
- GDPR was fashioned with a implicit assumption that a database is a centralized mechanism for collecting, storing and processing data; blockchains offer decentralized mechanisms for this.
- Does GDPR apply to blockchain?
    - GDPR applies to all personal data, regardless of the technology
    - Personal data is any information relating to an identified or identifiable natural person
    - It does not apply to anonymous data, but the threshold of what constitutes anonymous data is very high: must be able to irreversibly prevent identification
    - Pseudonymous data remains personal data under GDPR
- What data on a blockchain could be considered personal data?
    - **Transactional data**: including messages or any other content in the data
    - **Public keys:** here there is debate, but Finck believes they do constitute personal data under GDPR as they can be used to identify a person
- Article 29 Working Party has said that encryption is only pseudonymization so it remains personal data, and that hashing likely is too: hashed data remains personal data.
- Therefore assume if personal data is on a blockchain it is covered by GDPR
- Some important consequences and clashes with GDPR:
    - **Identifying the data controller:** At the application layer the data controller is the legal entity behind the app. At the infrastructure level more complicated, particularly in a permissionless context, where nodes would appear to be data controllers, which is problematic
    - **Transferring data out of the EU:** GDPR says you can only transfer third party data to a third country if it offers the same levels of protection; but in blockchain there is no control over where the data goes
    - **Data minimization:** GDPR says only process as much data as needed for a specific transaction; blockchains are ever-growing, append-only databases
    - **Right to amendment/erasure:** not possible in blockchains, which are in theory immutable and tamper proof

    - **Protection from automated processing:** not talked about much yet, but Article 22 gives data subjects the right to be protected from automated processing of information. How does that effect smart contracts?
- Many points of tension between this legal framework created under the assumption of centralized data collection and this decentral tech
- **Pessimistic conclusion:** There are many tensions and uncertainties between GDPR and blockchain and many blockchain projects are likely not compatible with GDPR. Some important people in GDPR, like Jan Philip Albrecht, have argued that DLTs are a threat to data protection, while many in the blockchain community are saying GDPR could be bad for innovation in Europe.
- **Optimistic conclusion:** Both GDPR and blockchain at heart share the objective of data sovereignty, so blockchain could become a tool to achieve this objective. Blockchain is also still an immature technology, so maybe could be shaped to be GDPR compliant, allowing us to have data protection by design.

Presentation - Alexis Berolatti - BCDiploma

- BCDiploma is offering a simple, blockchain-based solution to dematerialize the issuance of university and other degrees and easily allow individuals to prove they have the requisite certification.
- The project intentionally sought a public, permissionless blockchain and so uses Ethereum.
- To avoid centralization, the project chose to store all the data on the blockchain itself. However, was also clear to the project from the beginning that that could potentially conflict with GDPR.
- Therefore worked closely with the lawyers from the start to make the solution GDPR compliant.
- As importantly, BCDiploma created a data encryption technique that is they believe GDPR compliant, among other things by allowing for the right to be forgotten.
    - It makes use of AES 256 encryption and a special algorithm that ensures extra levels of encryption, as well as employing three keys, one for the graduate, one a diploma persistence key, and one a key from the issuing school.
    - All three keys are needed to encrypt the data. Students who choose to have their diplomas on the blockchain can choose with whom they share the information; if they want to be forgotten they can ask the issuer to destroy the persistent key, and the data can no longer be encrypted.

Panel discussion - Alexis Berolatti, Jörn Erbguth, Michèle Finck, Elizabeth Renieris

- Liability is a very important topic in this discussion. GDPR has a relatively hierarchical triparty model, with the data controller, data subject and data processor, with controller having ultimate controller. But the blockchain world is peer-to-peer, where individuals, entities and things become peers. In interpreting how GDPR and blockchain can reconcile themselves in this regard, you need to understand case by case what is happening to the data: how is it flowing, who is controlling what, who makes the decisions. Then you can better assess roles, responsibilities and liabilities under GDPR.
- In a blockchain, peer-to-peer world, it is possible for data subjects and data controllers to be the same entity, and the GDPR doesn't de facto stand in the way of this.
- There is a question of whether blockchains can really give data subjects control of their data when a) the technology is very intransparent, incomprehensible and hard to use for most people; and b) in a permissionless blockchain at least it is unclear who controls the network as ownership of mining/hashing power in the network can change over time, and perhaps fall to a 51% attack.
- Just as IP addresses have been deemed to be personal data in most *but not all* instances, encrypted data and hashes may not be personal data all the time. If they are used in a way that there is no reasonable way to break them, then they could be considered anonymized data and not fall under GDPR. But there are other issues as well in determining if something is personal data, including who has access to the private keys, whether or not personally identifiable can be gleaned from information extraneous to the key, and the fact that the Art 29 Working Party has said the perpetual nature of blockchains makes them pseudonymous.
- The issue of governance is one of the most important ones in this space. This issue can be very complex, as roles are fluid. Also not just about technical governance: off chain governance, especially where you have data or an oracle off chain, is equally crucial, as is industry self-governance.
- Looking at right to erasure, there have been conflicting legal opinions as to what erasure means: in one case, denying access (key destruction) was considered sufficient; in another, erasure was held to mean destruction of the data. Chameleon hashes and other techniques can be used to allow for modification of saved blockchain data, which can support the right to be forgotten. Architectures where the transactional data is separate from the personal data an also solve the problem by keeping personal data off the chain.
- Blockchain technology can directly support GDPR in different ways. There are different technical techniques, like chameleon hashes, zero knowledge proofs, and homomorphic encryption, that can be used to better secure personal data. Blockchain provides auditability and transparency, which can help in protecting data subjects and enforcing

GDPR, though these properties can also make it easier to personally identify data through inference. Blockchain can also greatly support GDPR's goal to improve the free movement and portability of data, and avoid data capture by large entities.
- Looking forward, among the most pressing questions that lawyers and technologists have to deal with is governance. Questions include who is the data controller in specific instances, but also who is controlling decentralized systems in general. We should not just focus on the tech but also on how it is employed, including considering the ethical choices we make when we use it.

Introduction: Claire Bury, Deputy Director General, DG CONNECT

- GDPR is timely now. The morning ended on an optimistic note. Let's take the positive momentum from this morning, starting from the assumption that blockchain can deliver the goal of data sovereignty, and find out how to do it.
- Are there ways to comply with data minimization, how far does the right to be forgotten extend, and most importantly: can Europe establish the right regulatory framework at the right moment? That is something we need to do swiftly and at scale if we want to lead in this area.

Roundtable discussion / Workshop

Topic 1: Technical solutions

Questions asked:

1. Is there a shared assumption that no encrypted data (reversible transformation) should be shared with 3rd parties, unless it is OK that they can decrypt it in the next 10 years?
2. What address obfuscation methods are acceptable?
3. What non-reversible data transformation methods are acceptable?
4. What are examples of successful implementations, out there in the wild?

Workshop answers:

- Principles / consensus agreed upon at the end of the working session:
    - In most cases putting PII on a blockchain is not advisable nor necessary
    - In practice it depends on the actual use case and the blockchain type
    - Obfuscation and data transformation methods are available, some of them in production (e.g. Ring signatures, Zero knowledge proofs, peppered hashes), they are more or less robust, none of them is perfect

    - Sovrin, Evernym, Decode are examples of successful implementations
- Questions left unanswered / where there is no consensus:
    - Are peppered hashes personal data or not?
    - Is it justified to use obfuscation and data transformation methods if they are robust for long enough (until the data becomes irrelevant)

Topic 2: Governance solutions

Questions asked:

Scenario 1: User using a platform that processes data with blockchain as backend

1. Are there any conceptual differences between Scenario 1 and the frameworks applied to traditional web services? Eg. app as the controller Eg. wallets, nodes, other services as processors

Scenario 2: User sends transactions directly or via transformation service

1. Can end-users be considered as controllers? can other actors be considered as processors?

Workshop answers:

- Principles / consensus agreed upon at the end of the working session:
    - A party can be both a controller for certain data, and a processor for other data (e.g. if data is only routed)
    - There is no unique answer regarding the status of nodes and it should be looked upon case by case
- Questions left unanswered / where there is no consensus:
    - None

Topic 3: Legal solutions

Questions asked:

1. What are examples of situations where the right to erasure can be waived, if any?
2. What best practices / things to avoid have you seen when it comes to consent and terms of service
3. What steps and procedures do you need to take determine if you / your teams are compliant with GDPR?

Answers given

- Principles / consensus agreed upon at the end of the working session:
    - You can't waive your right to erasure: however, it may not apply to the extent that processing is necessary for compliance with a legal obligation (e.g. KYC process in financial services)
    - In blockchain we need to find alternatives to erasure (e.g. not storing the personal data in the blockchain or making data inaccessible)
    - Consent has to be more than terms of services and should include the reality of the situation
    - Questions asked should be: What kind of data do I process? For what purposes? For how long do I need this data?
    - Portability is separate from erasure.
- Questions left unanswered / where there is no consensus:
    - Ask permission each time the data is processed by a smart contract is a possible best practice

Appendix

Official agenda

10:00 Opening DG CONNECT - Observatory & Forum Introduction - Olivier Micol, Head of Unit, DG JUST
10:15 Presentation - Michèle Finck: Blockchains and the GDPR
10:45 Presentation - Alexis Berolatti - BCDiploma
11:15 Panel discussion
14:00 Introduction Claire Bury, Deputy Director General, DG CONNECT
14:10 Working session - Part 1
15:15 Coffee Break
15:45 Working session - Part 2
16:50 Conclusion

List of registered participants

Niels Vandezande, Researcher - KU LEUVEN	Claire DEFLOU-CARON, President - GOVERSHIP
JEAN-MARC LECLERC, Government and Regulatory Affairs Executive - IBM	Leila Nassiri-Jamet, VP - GBA
Natalie Eichler, Associate - DWF	Katherine Hasiotis
Alexis Berolatti, COO - BCDiploma	Arnaud Le Hors, Senior Technical Staff Member - IBM
Florian Daniel, Senior Associate - DWF	Silvan Jongerius, CEO - TechGDPR
Chiara Dell'Oro, Adviser Retail Banking & Consumer Policy	Arthur Hilliard, EU Policy & Legal Professional
Sara Lipuzic, Legal Counsel Digitalisation - Shell	Adam Jones
Edwin Morley Fletcher, President - Lynkeus	Nadia Filali, Head of Blockchain - Caisse des Dépôts
Jordi Iparraguirre, Innovation Manager - EURid	Angeliki Dedopoulou - EC
Leonardo Vidal, Managing Director - Torlabix	Emmanuel Saliot - EU
Oliver Naegele, Founder - Blockchain-LAB	Alexandre Mateus - EC
Axel Beelen, Legal GDPR expert	Gabriele Mazzini - EC
Jörn Erbguth, Blockchain, Smart Contract and Data Protection (GDPR) Consultant	Fabrizio Sestini - EC
Carmen De la Cruz, Rechtskommission Co-Chair - swissICT	Fidel Santiago - EC
Thibault Verbiest, Legal Expert - DS Avocats	Anselm Rodenhausen - EC
	JACQUES Pascal - EC
	Jerome DETHIER - EC
	Lucile Collin - EC

Emilie Danglades-Perez, Lawyer - Simmons & Simmons Mohamed Chiboub Orangzeb Gohair Geo Van Langenhove, Legal Manager - EURid Cristina Carrascosa cobos - Chief Legal Counsel Udo Milkau, Director - DZ BANK Matijn Bolt, Freelance Blockchain implementation specialist Helene Benoist Carlos Pastor Matut, Digital Identity Leader - Alastria Anwar Soulami, Chairman - LifeBox ASBL Javier Sebastián - BBVA Elizabeth Renieris, Global Policy Counsel - Evernym Elizabeth Steininger, CEO - Least Authority Joachim Wilcke, Account Manager - FleishmanHillard Jean-Luc VERHELST, Bitcoin and Blockchain Author Valeria Ferrari Petrus van Steen Michèle Finck, Senior Research Fellow - Max Planck Institute; Keble College; University of Oxford	Adrian-Sorin Cristescu - EC Witte WIJSMULLER - EC Susana Nascimento - EC Robert Riemann - EU Peter Kerstens - EC Oscar Burgos - EC Omar Alam - EC NIETO MOREDA Luis Angel - EC Nada Milisavljevic - EC Mikolaj Jasiak - EC Marc-Antoine Lemaire - EC Fragkiskos ARCHONTAKIS - EC Gregory Steenbeek - EC Carmelo Zahra - EC Jean-Marie MISZTELA - EC marie-agnes deleglise - EC Camil Cristian LARGEANU - EC Birgit Hardt - EC Manuel Sanchez Jimenez - EC Martin le Vrang - EC Marian Cristian Vasile - EU Alina Senn - EC Gilles ROBINE - EC

Workshop slides

Available here

Workshop video

Available here

Related links and information

- EC GDPR site: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en
- European Data Protection Board https://edpb.europa.eu/edpb_en
- Opinion 05/2014 on Anonymisation Techniques: http://www.pdpjournals.com/docs/88197.pdf
- European Data Protection Supervisor Technologies Page: https://edps.europa.eu/data-protection/our-work/subjects/technologies_en
- BCDiploma website: https://www.bcdiploma.com
- BCDiploma white paper: https://www.bcdiploma.com/img/BCD-WhitePaper_last.pdf