www.jusletter-it.eu

Gabriel Jaccard / Adrien Tharin

GDPR & Blockchain: the Swiss take

The following paper addresses the main legal questions & best practices surrounding blockchain and GDPR. The Authors examine the legal challenges of storing personal data on a blockchain in a manner that complies with data protection regulation. In particular, the paper studies the question of personal data when it is considered anonymous, pseudonymous or encrypted on a blockchain. Further, it stresses the need for a legally efficient identity layer on the blockchain and digital systems in general. Finally, the paper addresses the question of the recognizability of the data controller & data processor within a blockchain ecosystem.

Category: Articles
Region: Switzerland; EU
Field of law: LegalTech; Data Protection

Citation: Gabriel Jaccard / Adrien Tharin, GDPR & Blockchain: the Swiss take, in: Jusletter IT 4 December 2018

ISSN 1664-848X, https://jusletter-it.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77 EDITIONS WEBLAW

Contents

I. Introduction

[Rz 1] The General Data Protection Regulation, or «GDPR»[1], will surely be one of the important cornerstones of an entire generation of lawyers. As of today, this important piece of legislation is the most detailed legal system aimed at protecting personal data.

[Rz 2] Historically, collection of personal data went through different phases of evolution, from the invention of devices enabling the capture of sound and images in the 19th century to the first methods of telecommunication in the beginning of the 20th century. At the time, the legal approach was to protect individuals through privacy rights. The invention of computers in the 1950s and the advent of internet gave way to the processing and collection of data, which have grown exponentially ever since. As a result, data protection regulation started to emerge and flourish[2].

[Rz 3] One of the latest developments is the emergence of blockchain technology as a storage system for personal data. The advantage of this technology is that the authenticity of stored data can be ensured. The downside is that, in order to be compliant with data protection regulations, blockchain systems may require complicated set up and the design of such systems has to be thoroughly carved out from the very first stages of their conception. This is also the reason why blockchain technologies represent a unique opportunity for data protection. Indeed, a General Data Protection Regulation (GDPR) compliant systems operating at an international level would enable a wider – *de facto* – adoption of this regulation, far outside the borders of the EU. Further, in certain cases, blockchain technologies enable users to gain control over their personal data, for example when such data is embedded in a digital token. In other words, because tokens can

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

2 https://www.weforum.org/agenda/2015/02/a-brief-history-of-big-data-everyone-should-read/ (all websites last visited on 20th November 2018).

be used to represent and identify specific data and because users are empowered with the use of private keys, digital data can become almost tangible.

[Rz 4] In this contribution, we will first give a very brief overview of the specifics of the blockchain technologies in light of the GDPR (*infra* n°II).We will then address certain specific issues relating to the application of GDPR within a blockchain ecosystem (*infra* n°III). Finally, we will present an executive summary and give a few key takeaways (*infra* n°IV).

II. GDPR & Blockchain

a. The Blockchain

[Rz 5] According to its most commonly accepted definition, the blockchain is a decentralized, distributed[3] digital ledger, that can be either private or public, which is used to record transactions. In one word, blockchain is a *database* and a subcategory of distributed ledger technologies (DLTs). The main advantages of using the blockchain is that records of information (i.e. data) cannot be altered retroactively without altering all subsequent blocks.

[Rz 6] However, there is not *one single* model of blockchain, but *many*. For instance, the blockchain's access to information may vary from completely accessible to the publicto absolutely private[4]. Public blockchains, since they are by definition publicly displayed, are often more problematic with regards to privacy laws and data protection[5] for a simple reason: once the identity of a user is known, it is possible to know the entire trail of activities and retrace its behaviour.

[Rz 7] In other examples, blockchain systems might abide by specific governance rules, i.e. granting certain advantages to given protagonists, such as voting rights and interests. This is particularly the case when a blockchain is related to a corporation, in which case there is a strong incentive and interest to control its development and decision-making process. Consequently, the result of any legal assessment about a blockchain system may vary strongly depending on how it is built[6].

b. GDPR's application in Switzerland

[Rz 8] The GDPR entered into force on the 25th of May 2018 and is directly applicable to its Member states and to any actors active within the European Union. According to its art. 3 al. 1, the GDPR shall also have an extraterritorial effect, since it applies to «*the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not*». In addition, the GDPR applies to controllers and processors outside the EU when their services are directed to European data

3 The word «replicated» would be technically more correct.

4 Ferreira Jesus Emanuel, Chicarino Vanessa R. L, de Albuquerque Célio V. N., de Rocha Antônio A., *A Survey of How to Use Blockchain to Secure Internet of Things and the Stalker Attack*, in : Security and Communication Networks Volume 2018, Article ID 9675050, available on https://www.hindawi.com/journals/scn/2018/9675050/, point 3.5.

5 Kosba Ahmed, Miller Andrew, Shi Elaine, Wen Zikai, Papamanthou Charalampos, *Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts*, in: IEEE Symposium on Security and Privacy 2016, p. 839.

6 Finck Michèle, *Blockchains and Data Protection in the European Union*, Max Planck Institute for Innovation & Competition Research Paper No. 18–01, November 30th 2017, p. 4.

subjects or when monitoring their behaviour (art. 3 al. 2 GDPR). In Switzerland, the Federal Data Protection Officer issued a statement indicating that Swiss corporations should consider that the GDPR applies whenever the data of an EU resident is processed[7]. Consequently, many Swiss companies and businesses sought to comply with those rules[8], and organized themselves to cooperate with European authorities[9].

[Rz 9] Switzerland, alongside with 12 non-EU countries, is also recognized as offering an adequate level of protection compare to the EU[10]. That allows personal data to be transferred to Swiss companies without having to comply with additional conditions set out in the GDPR, such as binding corporate rules or certification mechanism (art. 46 GDPR). Assessing the competent jurisdiction and the applicability of GDPR is of utmost importance in a blockchain's context. Indeed, the particularity of blockchain technologies, such as their decentralized network and potentially unrestricted use, make them easily fall within transnational data flow's scheme.

[Rz 10] In this vein, we note that blockchain's full nodes might often be located in multiples jurisdictions, which increases the difficulty to set the «blockchain's nationality» – i.e. the nationality of the data controller – or even to know from which jurisdiction and which nodes an outsourcing actually occurs. As a matter of legal consequence, the results of this situation is that the adequacy regime to be applied becomes utterly uncertain. In those hypotheses, we believe that one shall consider the outsourcing as occurring everywhere at the same time. Hence, as a matter of legal consequences blockchain would have comply with all the adequacy regimes all from the jurisdiction where the nodes are situated. This reasoning is motivated by the fact that the majority of nodes situated in one jurisdiction might change unpredictably over time, and that national data protection regime should not end up weakened by the use of blockchain.

III. Specific issues

a. Handling of personal data on the blockchain

1. What if personal data is stored on my blockchain?

[Rz 11] First of all, it should be stressed out that the question of whether the *access* to the data is private or public, i.e. whether the blockchain is public or private, is irrelevant. Indeed, data would generally be considered as processed under GDPR either way as long as personal data is processed. Further, the GDPR also applies to *filing systems*, which are defined as «*any structures set of personal data which are accessible according to specific criteria*, *whether centralised*, decentralised *or dispersed on a functional or geographical basis*» (art. 4 al. 1 nr. 6 GDPR). Consequently, the fragmented distribution of data and its public accessibility on blockchain technologies does not *per se* bar the application of the GDPR.

---

7 Préposé fédéral à la protection des données et à la transparence (PFPDT) of 1 January 2014, *Le GDPR et ses conséquences sur la Suisse*, mars 2018, p. 4.

8 *Idem*, p. 1.

9 With regards to the extend od this cooperation, please refer to: Benhamou Yaniv/Jacot-Guillarmod Emilie, *GDPR on the Swiss Territory Cooperation with European Authorities and Enforcement of Monetary Fines*, 2018.

10 See https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en.

[Rz 12] Secondly, the *type* of data is of great importance. Blockchain might handle *personal* or *non-personal* data. Both the GDPR and its Swiss equivalent, the Data Protection Act («DPA»[11]), apply only to *personal* data. As to *non-personal* data, some other important pieces of legislation can come into play, such as the proposed Regulation on a framework for free flow of non-personal data in the EU[12]. Hence, a blockchain handling exclusively non-personal data would fall under a comprehensively different and more permissible regime.

[Rz 13] Further between the different types of data, a distinction must be made as to whether the data stored on the blockchain is considered as *sensitive* (special categories of data within the meaning of art. 9 GDPR, such as biometric data, political opinions, etc.). In certain cases, biometric data is directly used to create a proof of digital identity (and self-sovereign identity) and will consequently require a higher level of protection. The degree of protection on the blockchain might differ depending on the data's format, such as document, plain text, hash code, etc. Most of the time, data on the blockchain is stored under hash coded format.

[Rz 14] Finally, the GDPR applies to the *processing* of personal data. According to art. 4 al. 1 nr. 2 GDPR, processing «*means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*». Since blockchains are in most cases ledgers[13] or databases, we can conclude that blockchain enters the definition of data processing.

2. Is a public key personal data?

[Rz 15] Basically, a public key is a numerical value that allows its holder to receive cryptocurrencies onto his account[14]. In blockchain systems, the public key is coupled with a private key according to the principle of asymmetrical cryptography. From a metaphorical point of view, a public key can be viewed as an address, in particular an IP address, keeping in mind that a single user may use numerous «accounts» or public/private keys, in a manner that is either permanent or non-permanent.

[Rz 16] The question of whether static IP addresses represent personal data was already decided at a European level[15]. In a few words: a static IP address should be treated as personal data depending on the ability to link the address with an identifiable person, considering all the means that may reasonably be put into place by the controller or a third party to identify the person who is linked to the data[16]. This can be the case, for instance, if one learns that some people has the

11 Federal Act of Data Protection of 19th June 1992 (FADP; CC 235.1).

12 See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017%3A495%3AFIN; Currently Awaiting Parliament 1st reading / single reading / budget 1st stage (http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2017/0228(COD)), Those data represent around 4% of EU GDP according to the the Free Flow Of Data Factsheet A4 FR 18th of September 2017.

13 Please note that some «ledgerless blockchain» recently appeared.

14 Romano Diego, Schmid Giovanni, *Beyond Bitcoin: A Critical Look at Blockchain-Based Systems*, in: Istituto di Calcolo e Reti ad Alte Prestazioni, I 80131 Naples, Italy, September 2017, point 3.2.1.

15 Judgement of the ECJ C70/10 (Scarlet) of the 24th November 2011, consid. 33.

16 Judgement of the ECJ C582/14 (Breyer) of the 19th October 2016, consid. 16 ff.

«address» XYZ (e.g. by entering an agreement), one could then retrace that person's behaviour from that information.

[Rz 17] In our opinion, along with other scholars, a public key should generally be regarded as personal data[17]. In particular, we believe that the link between the user and its public key, used in a permanent manner, is similar to the one relying a user with a *static IP address*[18] or even an email address.

[Rz 18] In the context of private blockchain, public keys might not always fall under the categorization of personal data, since users can be in charge of generating the sets of public/private keys and therefore, the burden of responsibility lies with the user[19]. In addition, it can be highlighted that the jurisprudence of the EU does not require the information enabling to identify a person to lie in one set of hands only[20]. Finally, a set of data may be considered personal data if the person that has access to this data has some legal possibility to obtain the identity of the data subject by reconciliating the information with other databases or information[21].

[Rz 19] Last but not least, the recognition of a certain statute for public/private keys holders might lead to conclude that there are some kind of property right, maybe partly similar to possession, over the digital asset/personal data linked to a public key.

3. Does «who is who» really matter on the blockchain?

[Rz 20] It does. But we see two possible angles to answer this rhetorical interrogation. The first one relates to the identity of the persons whose data is being processed. The second relates to the stakeholder's identity in order to govern the access, permissions, improve protection, or simply respect compliance requirements.

[Rz 21] The first key element to determine is *who is the data subject* and in which context. Indeed, the identity of the person concerned might raise some legal issues, e.g. if the person is below 18 years old (art. 8 GDPR). Further, the identity of the data subject might raise additional legal issues, for instance when the person qualifies as a consumer or as a Politically Exposed Person (PEP), since many additional rules as KYC/AML requirements or imperative jurisdiction rules[22], would then be applicable. New directives, such as the project of directive on the providing of digital content, might also apply[23]. As an example, according to its art. 2 al. 1 let. b, this directive applies to «*service allowing the creation, processing or storage of data in digital form, where*

17 See Reid Fergal, Harrigan Martin, *An Analysis of Anonymity in the Bitcoin System*, 2013; See Salmensuu Cagla, *The General Data Protection Regulation and the Blockchains*, Liikejuridiikka 1/2018; Ibáñez Luis-Daniel, O'Hara Kieron, Simperl Elena, *On Blockchains and the General Data Protection Regulation*, 2018, p. 5.

18 Judgement of the ECJ C582/14 (Breyer) of the 19th October 2016, consid. 16 ff. An IP address might be « static», i.e. that does not change between each of the connections, or «dynamic», i.e. the user is given a new IP address at each new connection. A dynamic IP address does not enable to make the link with the files accessible to the public between a certain computer and its address within a network of internet providers.

19 See Ibáñez / O'Hara / Simperl (Fn. 17).

20 Judgement of the ECJ C582/14 (Breyer) of the 19th October 2016, consid. 43.

21 Judgement of the ECJ C582/14 (Breyer) of the 19th October 2016.

22 Arner Douglas W, Zetzsche Dirk A., Buckley Ross P, Barberis Janos Nathan, *The Identity Challenge in Finance: From Analogue Identity to Digitized Identification to Digital KYC Utilities*, in: European Business Organization Law Review, Forthcoming; UNSW Law Research Paper No. 18–45; European Banking Institute Working Paper Series 2018 No. 28; University of Luxembourg Law Working Paper No. 2018-008, June 1 2018.

23 http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=fr&reference=2015/0287(COD).

such data is provided by the consumer». This will be of special concern to providers of Blockchain as a Service (BaaS) systems.

[Rz 22] Secondly, the question of the *storage location* – i.e. in which jurisdiction the full nodes[24] or the servers containing the data are situated is of utmost importance. When data is transferred outside of the EU – e.g. if one node is located in China – and especially towards countries with whom no adequacy decision exist[25], we would normally face a situation of international data transfer. The geographical location of the nodes was recently used by US courts to recognize its competence in the case Re Tezos Securities litigation, as part of the targeting test[26].

[Rz 23] On the question of the *applicable jurisdiction* in the context of a multinational processing of data, the GDPR relies on the «main establishment» (art. 4 al. 1 nr. 16 GDPR) of the controller, i.e. the place of central administration within the Union. The key here is to define where the essential of the processing of activities is taking place (see Recital nr. 36 GDPR), i.e. where the purpose and the means of the data processing are being determined. In the context of the blockchain technologies, we believe that when facing a situation where full nodes form jointly more than 50% of the decisional power at a moment t, they should collectively be considered as a controller within the meaning of the GDPR. When there is no central administration within the European Union, the notion of main establishment of the data processor (art. 4 al. 1 nr. 16 let. b GDPR) relies on the place where the main processing activities take place, to the extent that the processor is subject to specific obligations under the GDPR.

[Rz 24] In conclusion, we note that the legal assessment of blockchains requires the identification of its stakeholders for a variety of reasons. The concept of digital identity, especially when the processed have no legal relevance, has not yet been enough developed. In any case, the question of «who is who» is central to any legal or contractual relationships, and as a consequence we believe that no system handling personal data can be truly compliant without a legally relevant identification process[27].

4. What about Private data, Encrypted data, Pseudonymous or Anonymous data stored on the blockchain?

[Rz 25] In this section, we will assess the case of private data and encrypted data mostly under the EU legislation's perspective. For the basics of technical developments with regards to encryption methods please refer to Buchmann[28].

[Rz 26] First, let's study the case of *private data*, which can be described as data that is not made available to the general public, such as passwords and financial account details. Such data is often protected by various legal norms. For instance, professional secrecy (e.g. art. 321 Swiss Criminal Code[29]), banking information, or information covered by contractual agreement (e.g. non-disclosure agreements). Private data is not *per se* protected by the GDPR, hence we shall put

24 Full nodes represent a stakeholder within the blockchain who keep a full copy of the ledger and its protocols.

25 See art.13 ff. P-DPA.

26 See https://law.justia.com/cases/federal/district-courts/california/candce/3:2017cv06779/319743/130/.

27 Jaccard Gabriel, *Partie I : L'Identité Digitale et La Création Du Surhomme 2.0 (Part I: The Digital Identity and the Creation of the «Übermensch» 2.0)*, April 30, 2018; Salmensuu (Fn. 17), p. 9.

28 Buchmann Erik, *Anonymitätsmasse für Personendaten*, in: digma 2011, p. 166 ff.

29 Swiss Criminal Code (RS 311) of 1 March 2018.

it aside from our analysis. Even though, we may note that one of the Committee of the European parliament advised, in a preliminary report, that blockchain infrastructures should by default make sure that private data is being kept off-chain[30].

[Rz 27] Second, the case of *pseudonymous data*, which can be described as the processing of personal data in such a way that the personal data can no longer be attributed to a specific data subject without the use of additional information (art. 4 al. 5 GDPR). This type of protection is strongly recommended in the GDPR (Recital nr. 29 GDPR). The EU jurisprudence has stated that someone cannot be considered as identifiable if such an identification would be forbidden by law or not realizable in practice (e.g. disproportionate efforts in terms of time, cost, ...)[31]. Even when pseudonymised, data must be kept separately and technical and organizational measures must be taken to ensure that the data is not attributed to an identified or identifiable person. These different types of protection already exist within blockchain systems and are being used for pseudo-anonymization, like the use of hash functions to blind users identities[32].

[Rz 28] For instance, data is deemed pseudonymous if one uses of a number of control instead of a number of account[33]. Among pseudonymisation techniques, we can list encryption, hash-function, keyed-hash function with stored key, deterministic encryption or keyed-hash function with deletion of the key and tokenization[34]. We can notice that the use of hash still allows to link to an identity through comparison with the original file or whenever some specific patterns can be deduced from the analysis of the blockchain's paper trail; for instance, if the same hash was used multiple times before. Further, the process of encryption is a two-way function, meaning that with the right cryptographic key the process can be reverted to its original state i.e. reverse engineered. Finally, blockchain developers can develop multiple sets of keys or different techniques to encrypt data in such a manner that if one on the elements is stolen or corrupted, the whole trail and rest of data is no longer readable.

[Rz 29] Third, the case of *anonymous data*, which can be generally described as encrypted data, even though there is no formal definition in the GDPR. From a legal point of view, we should note that a perfectly anonymised set of data would in principle fall out of the scope of the GDPR[35].

[Rz 30] However, in order to be considered as anonymized under GDPR, the set of data must represent a near zero possibility to be linked to a person or entity, which is as of today technically impossible to assure. Indeed, anonymous data requires *irreversibility*, which disables the possibility to process the personal data. As highlighted by Salmensuu, this process aims at preventing the singling out of an individual in a dataset, from linking two records within a dataset and from inferring any information in such dataset[36]. We believe that this requirement can be criticized since a level of security that is too high is detrimental to research and analysis of databases. Also, re-

30 Committee on International Trade, *Draft report on Blockchain: a forward-looking trade policy (2018/2085(INI))*, of 18th July 2018, point 22.

31 Judgement of the ECJ C582/14 (Breyer) of the 19th October 2016, consid. 46 ff.

32 https://www.hindawi.com/journals/scn/2018/9675050/.

33 Swiss Federal Court decision 4A_365/2017 of 26th February 2018, consid.5.3.1.

34 WP 2014 Opinion 216, p. 21; see also Nchinda N., *Exploring Pseudonimity on Ethereum*, https://media.consensys.net/exploring-pseudonimity-on-ethereum-dda257019eb4

35 Recital 26 Articles 4 and 5 of the GDPR, Salmensuu (Fn. 17), p. 14.

36 WP 2014 Opinion 216, p. 9.

quiring a near-zero possibility of identification seem excessive in light of the EU jurisprudence[37], as the required level of protection is not absolute (see below).

[Rz 31] Even though the anonymization or pseudonymisation of data can present some data transparency concerns[38], they are still very useful tools. For instance, a breach following the release of unintelligible data (e.g. encrypted data under art. 34 al. 1 let. a GDPR) does not trigger notification obligation to the data subject.

[Rz 32] Last but not least, the possibility to identify someone with data, may be seen as an absolute or relative concept[39]. Consequently, some doctrinal opinions, which believe in the absolute concept, have stated for instance that registering personal data on a blockchain would never be compliant since the rise of quantum computer or other technologies might be able to break it someday. We believe this opinion to be considered as excessive, since the Recital 26 of the GDPR refers only to «*all the means reasonably likely to be used*» by the data processor or by a third party. In addition, the GDPR states that the technical measures to protect the data must be appropriate and depends on the current technical state of the art, the type of treatments and the risk (art. 25 RGPD; art. 6 P-DPA[40]).

[Rz 33] In Switzerland, it is interesting to note that the approach with regards to the encryption of data would probably be slightly different. Recently, the Swiss Federal Court 4A_365/2017 of 27th March 2018, stated that identifiability depends on the concrete elements of the case, i.e. where the technical possibility, the efforts needed and also the personal interests of the data processor or any third party to discover the real identity behind the personal data need to be taken into account[41].

[Rz 34] Finally, we might highlight that a few GDPR-compliant solutions to process personal data already exist. First, the use of *zero-knowledge proof protocol*[42]. A zero-knowledge protocol is a method by which one party can prove to another party that something is true, without revealing any information apart from the fact that this specific statement is true. This method gives a near 100% statistical probability of not revealing the identity of this party. Note however that the use of a zero-knowledge proof mechanism also enters the definition of data processing[43].

[Rz 35] A second way, would be to use secure *multi-party computation*, where data is split between different nodes, which compute functions together without leaking information to other nodes. More specifically, no single party ever has access to the data in its entirety; instead, every party has a meaningless piece of it. This results from the so-called millionaire's problem proposed by Yao[44].

---

37 In particular, in view of the Breyer's jurisprudence (Judgement of the ECJ C582/14 (Breyer) of the 19th October 2016); Salmensuu (Fn. 17), p.21, Recital 26 GDPR.

38 Committee on International Trade, *Draft report on Blockchain: a forward-looking trade policy (2018/2085(INI))*, 18th July 2018, p. 9.

39 Salmensuu (Fn. 17), p. 15 ff.

40 Message P-DPA, FF 2017 6593.

41 Decision Swiss Federal Court 4A_365/2017 of 26th February 2018, consid. 5.

42 http://www.cs4fn.org/security/shafigoldwasser.php.

43 Decision Swiss Federal Court 4A_365/2017 of 26th February 2018, consid. 5.2.2 «*Diese Daten anonymisiert bzw. pseudonymisiert, bearbeitet sie diese grundsätzlich geschützten Daten im Sinn von Art. 3 lit. e DSG, auch wenn das Resultat dieser Bearbeitung keine Personendaten bzw. geschützte Daten mehr sind*».

44 Two millionaires are interested in knowing which of them has the largest fortune without revealing their own to another or to third parties Yao A. C., *Protocols for secure computations*, in: Proceedings of the Foundations of Computer Science, 1982.

[Rz 36] Thirdly, we can also mention other mechanisms, as for instance are ring signature[45], Enigma's private smart contract[46], etc.

[Rz 37] In conclusion, we believe that the data storage of personal data should use a combination of on-chain/off-chain mechanisms[47], for instance blockchain systems limiting the use of personal data on-chain by using personal data encrypted within an external server (off-chain)[48].

b. Who is the data controller & processor?

[Rz 38] The definitions of data controller and *a fortiori* data processor aim at determining an official point of contact and intermediary to ensure the application of the GDPR. Indeed, one of the key purposes of the law is to avoid the possibility of having data processed without any accountabilities (e.g. art. 5 al. 2 GDPR). As an example, we can highlight the obligation in certain situations to designate a data protection officer (DPO) in order to ensure this objective (art. 37 GDPR).

[Rz 39] The data controller is defined as «*the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law*» (art. 4 al. 1 nr. 7 GDPR). Whereas the processor is «*a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*» (art. 4 al. 1 nr. 8 GDPR). Stakeholders in a blockchain may either fall in one category or the other. Finally, the Swiss system follows a similar approach in the P-DPA (see in details)[49].

[Rz 40] Blockchain infrastructure implies a multitude of stakeholder, therefore we must differentiate between the types of actors and their roles, which might all be implicated into the processing of data with different liabilities[50]. In the blockchain context, the person that are often implicated and the most relevant in our analysis are either the developer of the blockchain, the full nodes and the simple nodes of the blockchain[51]. Finally, it is important that we define full nodes, i.e. stakeholders that have the full copy of the blockchain, while light weighted nodes only perform certain operations and only have the hash code of the blocks.

45 https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/.

46 https://enigma.co.

47 Sater Stan, *Blockchain and the European Union's General Data Protection Regulation: A Chance to Harmonize International Data Flows*, November 6, 2017, p. 30; see also Finck (Fn. 6).

48 Those solutions were further developed in Zyskind G., Nathan O., Pentland A. S., *Decentralizing privacy: Using blockchain to protect personal data*, in: Proceedings of the IEEE Security and Privacy Workshops, SPW 2015, pp. 180–184, IEEE, May 2015.

49 PFPDT (Fn. 7), p. 4 s.

50 Judgement of the ECJ C-210/16 (Wirtschaftsakademie) of the 5th June 2018, points 28, 43 f.

51 Other actors, such as miners are to be considered but we will not focus our analysis on those stakeholders.

1. Data controller

[Rz 41] The notion of data controller is threefold and includes first an entity («*natural or legal person*»), second a pluralist liability («*alone or jointly*»), thirdly the essential characteristics of the activity («*determines the purposes and means*»).

[Rz 42] Let us assess the first condition. We can say that from every full node composing the blockchain, it is always theoretically possible to identify at least one natural or legal person. Further, the conditions of what may constitute a legal or natural person relies on the competence of the member state. Consequently, there is potentially some leeway into this definition. Furthermore, the qualification of the property rights between a token and its holder, as well as with its private/public key in civil law is in constant evolution. In particular, it would be possible that one of the member states recognize token holders or nodes as forming a joint corporation having some kind of property rights over the blockchain. In Switzerland, there is a debate around the qualification of decentralized applications (DApps) and blockchain community as general partnerships[52]. In our view, the qualification of most – traditional – blockchain platforms as a general partnership under Swiss law is convincing. Indeed, the full nodes contribute with specific abilities and/or capital for a specific purpose.

[Rz 43] The GDPR defines the terms «*enterprise*» as a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity within the EU. We can note that in the jurisprudence of the CJEU, the qualification of data controller is a bit blurred. For instance, in one of its decision, the CJEU recognized that members of a religious community have been found jointly, but with a difference of degree[53], as data controller[54]. Consequently, we do believe it is possible to consider full nodes as entities capable of being subject to the GDPR.

[Rz 44] In the event full nodes were not considered liable under GDPR, we believe there is an obligation relying on the blockchain designer, i.e. the corporation or natural person setting the blockchain, to comply with the GDPR. In case of token generating events (TGEs, ICOs), where a blockchain will be set as completely public, we believe the first designers shall be considered as the first data controller that could be held liable for certain damages and responsible for the respect of certain obligations (such as designating a DPO (art. 37 GDPR). Absent the possibility to determine one or data controllers at a later stage, the designers of a blockchain should keep in mind the obligation under the GDPR to create a system that compliant by design and by default with data protection (art. 25 GDPR; art. 6 P-DPA). Therefore, authorities or private parties could be tempted to hold them liable.

[Rz 45] Second, we will assess the second and third characteristics (joint processing & determination of purpose).

[Rz 46] The *joint processing* of data is particularly interesting in the blockchain context, since the whole principle of a decentralized database is to disperse the information into a network. The case of joint controlling (art. 26 GPDR) involves that the nodes have to organize in a manner that determines their respective responsibilities for the compliance with the obligations under the GDPR, like the designation of a contact point for data subjects. In this regard, we can state

52 See Gyr Eleonor, *Dezentrale Autonome Organisation DAO*, in Jusletter 4. Dezember 2017.

53 Judgement of the ECJ C-25/17 (Jehovah) of the 10th July 2018, point 66.

54 Judgement of the ECJ C-25/17 (Jehovah) of the 10th July 2018.

that the qualification of joint controlling of the full nodes of the blockchain is acceptable under EU law.

[Rz 47] The determination of purpose is relevant to the notion of *control* over data, which means making a decision about why and how a particular data processing activity takes place[55]. The effective power over the processed data and the qualification of controller may even result from the objective perspective of the person whose data are being processed[56]. Further, we can see the approach taken of this notion is factual, as stated by the W29 committee[57], and is described in the jurisprudence of the EU as «*a natural or legal person who exerts influence over the processing of personal data, for his own purposes, and who participates, as a result, in the determination of the purposes and means of that processing, may be regarded as a controller*»[58]. For instance, this reasoning was applied to qualify the administrator of a Facebook page as data controller[59].

[Rz 48] As a result, we can see three alternative solutions arising from the above legal considerations with respect to blockchain:

[Rz 49] First, all full-nodes qualify independently as data controllers[60]. This solution would not be compatible with the GDPR, since no nodes has an effective control over the blockchain.

[Rz 50] Second possibility, full nodes may qualify as data controller when they jointly represent a combined decision power of > 50%. In order to be applicable, the GDPR or an execution decision exercised toward the blockchain, shall have jurisdictional control and competence over at least this proportion of nodes or the legal or natural person by whom they are managed. In the event that some of the full nodes are located within the EU but represent < 50% we can wonder whether this minority shall take an active role into taking some active measure into making the blockchain compliant, notably in case of a hard fork.

[Rz 51] Third possibility, no nodes qualify as a controller[61] at the *t* moment the observer is looking at the blockchain. In those cases, as mentioned above, we believe that the relevant point would be the moment of the creation of the blockchain to attach some obligation and liability to the designer, since the GDPR imposes privacy by design and by default. Consequently, the blockchain developer must carve out in the design system that complies with data protection resulting if needed into appointing of a DPO with special editing power over the blockchain.

[Rz 52] Finally, even in the hypothesis where a liable data controller would be singled out, the execution of the GDPR's sanctions would be uncertain. For instance, what would happen if the Bitcoin blockchain was considered GDPR non-compliant? The first difficulty would be to identify the legal or natural persons behind the full nodes. The second would appear in the eventuality the full nodes in the EU's jurisdiction do not have actual control over the blockchain's processing. In this later case, an *exequatur* of the decision would have to be seeked in the foreign jurisdictions where full nodes have been identified. And last but not least, a third problematic aspects would be to decide whether full nodes, which are situated outside of the EU and does not qualify as a

55 WP 2010 Opinion 169 p. 8.

56 Judgement of the ECJ C-25/17 (Jehovah) of the 10th July 2018, point 21 ff.

57 WP 2006 Opinion 128.

58 Judgement of the ECJ C-25/17 (Jehovah) of the 10th July 2018, point 68.

59 Judgement of the ECJ C-210/16 (Wirtschaftsakademie) of the 5th June 2018.

60 See also : Ibáñez / O'Hara / Simperl (Fn. 17), p. 5.

61 Berberich Matthias, Steiner Malgorzatta, *Practitioner's Corner Blockchain Technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers?*, 2016, p. 425.

data controller, would have to be sanctioned next to a data controller? In other words, would all the stakeholders of the non-compliant blockchain be severally liable? We believe that a drastic answer to either of those questioning would probably slow down blockchain adoption, encourage anonymity and possibly create more scission and forks among blockchain communities.

2. Data processor

[Rz 53] The first condition refers to a legal or natural person. Consequently, we may refer to the above section.

[Rz 54] The second condition is the processing of personal data on behalf of the data controller. In this regard, we note that the jurisprudence of the EU retains that instruction, or guidelines, do not need to be in written form[62]. In our view, the blockchain protocol, where the rules for processing are set, would be hence a sufficient instruction. Further, those rules are always taken jointly by an entity who had initially or has at the moment of the adoption/modification of the protocols rules a factual power of decision, hence qualifying as data controller[63]. In particular, the EU jurisprudence does not require that the data processor have even access to the personal data to be implicated into his liability[64].

[Rz 55] Consequently, every full nodes (along with miners[65] probably) would qualify as a data processor under GDPR. Even further, every lightweight node might also qualify as such since they also fall under the regulation of the protocol. This approach is in accordance and comparable with today's qualification over internet's stakeholders, service providers, hosts, etc. In particular, we believe the activity of full nodes could be in essence compared to internet hosting.

c. Data portability

[Rz 56] The right of portability of the data is one of the GDPR specificities, which was not followed by Switzerland[66]. This is the reason why we will simply mention its existence without further developments. In regards of the blockchain, we can say that data portability represents a detrimental challenge since this right requires, to be meaningful, the interoperability of the systems in-between different blockchain, which is something that does not yet exist in practice, notably due to the lack of standardization.

d. Right to be forgotten

[Rz 57] The right to be forgotten, or right to erasure, is set out in art. 20 GDPR. It creates a new right for the data subject to force the data controller to permanently erase or restrict any data held by the controller.

---

62 Judgement of the ECJ C-25/17 (Jehovah) of the 10th July 2018, point 67.

63 See also: Ibáñez / O'Hara / Simperl (Fn. 17), p. 5.

64 Judgement of the ECJ C-210/16 (Wirtschaftsakademie) of the 5th June 2018, point 38; see also Salmensuu (Fn. 17), p. 25.

65 See Ibáñez / O'Hara / Simperl (Fn. 17), p .4.

66 Message P-DPA, FF 2017 6593.

[Rz 58] In short, we follow the doctrinal opinion that, according to the principle of functional equivalence[67], the act of disabling access to personal data should be considered as erasure by law[68]. Also, in the event where personal data can be processed in a way that is equivalent to complete anonymization, it should also be considered as erasure. In particular, when the processed methods respects the so-called *forward secrecy*; i.e. when the decryption keys are destroyed immediately after use[69]. Furthermore, the doctrines is keen to consider even a «*sufficiently strong encryption scheme*»[70], as an acceptable mean to accomplish erasure. In our view, this opinion has solid argument, notably in the view of the jurisprudence Breyer[71], which excludes a totally absolute requirement of cryptographic security.

[Rz 59] If the principle of functional equivalence was not retained, the right of erasure would then require to set a mechanism of «*golden key*» within the blockchain[72], which means the ability to edit it after the chain was validated. We believe this would reintroduce an element of centralization into the blockchain governance, hence depriving the blockchain of its *raison d'être* and contradicting its very own purpose and conception. Such a system could be implemented, in the case of a public blockchain by having one or several designated entities or full nodes; whilst in private blockchain the keys could be hold collectively by the principal stakeholders[73]. Finally, we don't believe that the personal data subject shall be directly empowered with a golden key over its personal data as it would be impracticable[74].

e. The importance of self-regulation & standards

[Rz 60] Last but not least, one of the themes that is almost never treated is the importance that is left to self-regulation and the creation of standards. Indeed, the compliance with the law is likely to be much influenced by the harmonization of technical standards developed by private parties be it at international or at the European level. We will especially refer to the importance given to the technical standards in the GDPR (e.g. Recital 28 Directives on certain aspects concerning contracts for the supply of digital content[75]). Also, the European Committee on trading has highlighted that the Commission shall have an active role, and contribute to the creation of those standards, notably with regards to the security of data[76].

67 E.g. presented by Furrer: https://www.mme.ch/en/magazine/magazine-detail/url_magazine/functional_equivalence_of_digital_legal_transactions/.

68 Salmensuu (Fn. 17), p. 24.

69 Abelson Harold et al., *Keys Under Doormats: mandating insecurity by requiring government access to all data and communications*, 7th of July 2015, p. 3.

70 See Ibáñez / O'Hara / Simperl (Fn. 17), p.8.

71 Judgement of the ECJ C582/14 (Breyer) of the 19th October 2016.

72 Abelson, p.1; Costa Pier Francesco, *Ethereum blockchain as a decentralized and autonomous key server: storing and extracting public keys through smart contracts*, 2016, p. 40.

73 Sater (Fn. 47), p. 36.

74 For instance, see Ouaddah et al., *FairAccess: a new Blockchain-based access control framework for the Internet of Things*, in Security and Communication Networks, vol. 9, no. 18, pp. 5943–5964, 2017.

75 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52015PC0634.

76 Committee on International Trade, *Draft report on Blockchain: a forward-looking trade policy (2018/2085(INI))*, 18th July 2018, point 24 f.

IV. Conclusion

[Rz 61] In conclusion, the authors of this contribution believe that blockchain technologies offer a unique, but yet underestimated opportunity to enforce the rights and obligations introduced by the GDPR. Developers should try to implement GDPR compliance from the early stages of conception of their product rather than once the technology, code, platform or smart contract is deployed. It is however difficult to predict all its possible uses and evolutions of these products and in certain cases, adjustments may be needed along the way. However, many systems do not allow such adjustments without disproportionate efforts and some of them are simply impossible to change. This is the consequence of the purpose of blockchains to serve as immutable, hence reliable, databases.

[Rz 62] As a few summarized takeaways:

- GDPR applies to public and private blockchains;
- «Sensitive» data, such as biometric, health or genetic data stored on the blockchain need extra levels of security;
- Blockchain technologies enter the definition of «processing» in the meaning of GDPR;
- A public key can be considered as personal data if the identity of its holder can be determined by reconciliation with other data;
- Other types of regulation, such as anti-money laundering or consumer protection laws, might apply depending on the nature of the information stored on the blockchain;
- Pseudonymisation and anonymization can be a solution to avoid triggering data protection obligations;
- Full nodes could in principle be considered as joint data controllers in the sense of the GDPR and full nodes and miners individually could qualify as processors;
- Obligations of privacy by design and privacy by default should be taken into account when creating a new blockchain; absent joint data control of the full nodes, developers and designers of a blockchain could be held liable;
- Designating a DPO from the earliest stages of development of a blockchain technology should be mandatory;
- Right to portability seems impossible to put in practice between blockchains, at least under the current state of technology;
- Complete erasure from the blockchain is impossible. However, complete removal of the access to personal data or irreversible anonymisation of personal data should be considered as tantamount to erasure;
- Ability to edit the blockchain at a later stage would simply defy the very purpose and definition of blockchain.

Gabriel Jaccard holds a BLaw from the University of Fribourg and a MLaw from the University of Zurich. Currently, M. Jaccard is a PhD candidate at the University of Geneva. His thesis focuses on the private law issues relating to blockchain in general and smart contracts in particular.

Adrien Tharin specializes in data protection, intellectual property, privacy law and all matters related to the internet, media, entertainment and legal tech industries. He also practices in commercial and corporate law as well as in immigration law matters. Earlier in his carrier, Adrien has gained a solid experience in domestic and international litigation, particularly in commercial

and banking disputes and white-collar crime. He holds a LL.M. from University of California, Los Angeles and a LL.M. from the Institute for European Studies of the Université libre de Bruxelles. Adrien has also made many publications, notably in Le Temps.