www.jusletter-it.eu

Rolf H. Weber

The Interplay of Blockchain Technologies and Data Protection

The new technological infrastructures such as blockchain cause challenges in respect of compliance with the continuously stronger data protection principles around the world. Particularly the relatively strict data privacy provisions in Europe have a substantive impact on blockchain business models. This contribution analyses the manifold (but mostly not unsurmountable) tensions caused by blockchain characteristics to data protection objectives and outlines to what extent distributed ledgers can also serve as privacy-enhancing tools.

Beitragsart: Blockchain
Region: Schweiz; EU
Rechtsgebiete: Blockchain; Datenschutz

Zitiervorschlag: Rolf H. Weber, The Interplay of Blockchain Technologies and Data Protection, in: Jusletter IT 30 September 2020

Contents

1. Introduction
2. Basic Regulatory and Technological Framework
    2.1. Scope of Application of Data Protection Laws
    2.2. Protection of Personal Data
    2.3. Anonymization and Pseudonymization Issues
3. Controller and Processor
4. Key Principles of Data Protection
    4.1. Lawfulness and Transparency
    4.2. Purpose Limitation
    4.3. Data Minimization and Storage Limitation
    4.4. Data Subjects Rights
        4.4.1. Right to Rectification
        4.4.2. Right to Erasure / Right to be Forgotten
        4.4.3. Right to Data Portability
        4.4.4. Right against Automated Data Processing
5. Blockchain as a Tool for Improving Data Privacy Objectives
    5.1. Technological Developments
    5.2. Blockchain as Privacy-Enhancing Tool
    5.3. Policy Options
6. Outlook

1. Introduction

[1] The term «blockchain» is commonly used as description of a specific type of distributed ledger technology (DLT). So far, a generally accepted definition is not existing; the International Organization of Securities Commissions (IOSCO) understands DLT as a «consensus of replicated, shared, and synchronized digital data geographically spread across multiple sites, countries, and/or institutions».[1] Therefore, a DLT is a combination of peer-to-peer networking, cryptography and distributed data storage; blockchain should be seen as a decentralized infrastructure system in the form of a continuously growing list of records that are linked and secured by use of cryptography.

[2] Blockchain can be implemented in different technological designs, for example as private or public, and as permissioned or permissionless infrastructure; in all cases, however, the blocks hold badges of valid transactions that are hashed or encoded.[2] The use of blockchain technology is open to many segments of the society and economy; at the beginning the finance markets have been at the forefront (and it appears still to be), but in the meantime supply chains (following the efforts of the OECD to promote blockchain as part of responsible business conduct) as well as applications in the governmental context gained some importance.

[3] Data protection laws are strengthened around the world. The General Data Protection Regulation (GDPR) of the European Union is often seen as the most ambitious legislation for

[1] IOSCO, Research Report on Financial Technologies (Fintech), 3 February 2017, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD554.pdf, 51.

[2] See amongst others Primavera De Filippi/Aaron Wright, Blockchain and the Law. The Rule of Code, Harvard University Press, Cambridge MA 2018, 76; Dan Tapscott/Alex Tapscott, The Blockchain Revolution, Random House, New York 2016, 75; Rolf H. Weber, Regulatory Environment of the Ledger Technology, Computer Law Review International 2017, 1.

data privacy; therefore, the GDPR will be the key reference in this article.[3] Switzerland has also adopted a new Data Protection Act (DPA) on 25 September 2020 which is considered to be equivalent but not identical to the GDPR.[4] In principle, the challenges caused by blockchain technologies to the existing data protection framework can best be analyzed by discussing a quite strict data privacy regime.

[4] Since tensions can occur between the blockchain technologies having emerged as a «revolutionary» infrastructure for digital transactions and new privacy rights, the need has become apparent to address the relevant issues in a detailed way.[5] The respective challenges are increased in view of the fact that – as mentioned – blockchain is able to serve various possible uses. At the outset, the following tensions can be identified: (i) Whereas data protection provisions contain clear responsibility rules (controller, processor), the blockchain technology realizes distributed responsibility and anonymous participation. (ii) Whereas data protection laws embrace several individual privacy rights, the (public) blockchain is not designed to implement personalized «values».

[5] Notwithstanding the fact that technology neutrality on the blockchain causes data protection challenges, the following contribution argues that DLT or blockchain technologies offer a unique, but yet underestimated opportunity to enforce privacy rights. IT developers do have the means to implement privacy laws' compliance into the concept of their products and services (for example privacy by design / privacy by default). Since the blockchain is immutable, the databases remain reliable if designed appropriately in their early stages.

[6] However, several research questions need to be tackled, for example:[6] (i) Is a public key a personal data? (ii) Does «who is who» matter on the blockchain? (iii) Can anonymous or pseudonymous data be stored on the blockchain? (iv) Who is the controller and/or processor of data? (v) What about the right to erasure or the right to portability? In view of the given legal uncertainties it is worth addressing the mentioned legal challenges hereinafter.

[3] Regulation (EU) 2016/679 of 27 April 2016,OJ L 119/1-88 of 4 May 2016; as far as the «frontrunner» function is concerned, the highly acknowledged American Journal of International Law (AJIL) devoted a whole issue in Vol. 114 (2020) to the topic of «GDPR and International Law» (seven contributions), discussing amongst others the question whether the GDPR can be qualified as global regulation (edited by Cedric Ryngaert/Mistale Taylor).

[4] The Swiss DPA was adopted on 25 September 2020 (subject to a potential referendum); hereinafter, the provisions of the draft bill of the DPA as submitted by the Federal Council to the Parliament (Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz of 15 September 2017, BBl 2017, 6941 et seq.) are cited; the discussed provisions have not been subject to major changes during the parliamentary processes but their numbering might deviate (mainly from Art. 16 onwards).

[5] See European Parliament, STOA, Panel for the Future of Science and Technology, Blockchain and the General Data Protection Regulation, Study, July 2019, available at http://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf (hereinafter STOA-Study); Michael Isler, Datenschutz auf der Blockchain, Jusletter, 4 December 2017; Cornelia Stengel/Roman Aus der Au, Blockchain: Eine Technologie für effektiven Datenschutz?, sic! – Zeitschrift für Immaterialgüter-, Informations- und Wettbewerbsrecht 2018, 439 seq.

[6] See also Gabriel Jaccard/Adrien Tharin, GDPR & Blockchain: The Swiss Take, Jusletter IT, 4 December 2018, nos. 11 et seq.

2. Basic Regulatory and Technological Framework

2.1. Scope of Application of Data Protection Laws

[7] The territorial scope of data protection laws is regularly defined in a broad way. The data protection principles and requirements obviously apply if the controller or the processor has an establishment in the concerned jurisdiction. «Establishment» means the execution of any real and effective activity through a stable arrangement. In addition, based on a functional approach, the provisions also are applicable if the subjects of the data collection or processing are located in the jurisdiction.[7] In the EU, the provider of services on a blockchain is exposed to the GDPR as soon as it cannot be excluded that these services are directed to EU persons. Furthermore, the monitoring of the behavior of an EU person equally leads to the application of the GDPR. In a nutshell, due to the regularly broadly understood territorial scope (also in Switzerland) it appears to be highly likely that the applicable data protection law has an (almost) global reach in the blockchain context.[8]

[8] The material scope of data privacy in the EU is defined by «the processing of personal data wholly or partly by automated means and to the processing of other than automated means of personal data which form part of, or is intended to form part of, a filing system» (Article 2(1) GDPR). The term «processing» is also widely described as «any operation or set of operations which is performed on personal data or sets of personal data» (Article 4(2) GDPR; similarly Article 4(d) DPA). In principle, blockchain-enabled data processing qualifies as data processing by automated means.[9] Therefore, services' offerings on the blockchain by a foreign entity are very likely falling into the scope of application of the concerned data protection law.

2.2. Protection of Personal Data

[9] The starting point for the applicability of data protection laws is the term «personal data». Most laws have adopted a binary perspective between personal data and non-personal data. The definition of personal data in Article 4(1) GDPR and in Article 4(a) DPA is quite inclusive and not only covers any information relating to an identified natural person, but also any information relating to an identifiable natural person in a direct or indirect way.[10] With the new techniques (mainly big data analytics) a person is rather easily identifiable, even if a clear drawing line between the two categories is difficult to establish.[11] Therefore, in view of the broad understanding of identifiability the term «data» relating to a data subject is usually to be considered as information about that individual.[12] As a result, in order not to violate the data protection principles,

[7] Art. 3(1) and (2) GDPR; see also European Court of Justice (ECJ), Case C-230/14 Weltimmo (2015), EU:C:2015:639, para. 28; Case C-131/12 Google Spain (2014), EU:C:2014:317, para. 52. The Swiss legislator has decided not to introduce an explicit provision on the geographical scope into the DPA since jurisprudence has already decided that the effects principle of international law will be applicable (BGE 138 II 346 E. 3.3, Google Street View).

[8] STOA-Study (supra n. 5), 9.

[9] See also EJC, Case C-101/01 Bodil Lindqvist (2013), EU:C:2003:596, para. 25.

[10] Article 29 Working Party, Opinion 04/2007 on the concept of personal data (WP 136), 01248/07/EN, 6/7; from the court practice see Joined Cases C-141/12 and C-372/12 YS v. Minister voor Immigratie (2014), EU:C:2014:2081; Case C-434/16 Nowak (2017), EU:C:2017:994.

[11] STOA-Study (supra n. 5), 16/17.

[12] Consequently, the notion «personal data» is only not fulfilled in case of a complete anonymization of the data.

data should be anonymized. So far, such kind of transformation from personal to anonymized data is based on standards envisaging to avoid the identifiability of a person.

[10] The previous data protection supervisory authority of the EU (namely the Article 29 Working Party) has developed three different criteria to be considered in order to determine whether a de-identification is «irreversible» or «as permanent as erasure».[13] It must be assessed whether (i) it is still possible to single out an individual, (ii) it remains feasible to link records relating to an individual, and (iii) the information concerning an individual can still be inferred. The respective Opinion 05/2014 of the Article 29 Working Party on «Anonymization Techniques» contains further information about the assessment criteria for the consideration of identifiability.[14] Transforming personal data in a manner that excludes any singling out, link-setting and inference in a reasonable manner is quite difficult in reality.

[11] In a given case, an objective rather than a subjective approach must be applied in order to meet the criterion of the – in the UK terminology – «motivated intruder».[15] In addition, usually the dimension of time is to be considered as well as the question of the individual or entity holding the personal data. Further guidance can be drawn from the fundamental rights framework (right to privacy and informational self-determination) as concretized by international and national constitutional courts.[16]

[12] A private key obviously is personal data since it identifies the entitled holder of the key, similarly as a password. But also a public key can become personal data if it has the function of an identifier, i.e. if it enables the identification of a specific natural person in practice (and possibly also reveals a pattern of a transaction).[17] A public key as a numerical value is similar to an IP address; already several years ago, the Swiss Supreme Court and the European Court of Justice expressed the opinion that a static IP address must be treated as personal data depending on the ability to link an address with an identifiable person.[18] The link between the user and its public key, applied in a permanent manner, is comparable to the situation of a static IP address. In 2016, similar assessments have been made in respect of a dynamic IP address.[19] Only in case of a private blockchain, public keys might not always fall into the category of personal data since users can be entitled to generate sets of «public/private» keys leaving the identification task with them.[20]

2.3. Anonymization and Pseudonymization Issues

[13] Not directly related to the blockchain environment, anonymization techniques are encryption, hash-function, keyed-hash function with stored key, deterministic encryption or keyed-hash

[13] Article 29 Working Party, Opinion 05/2014 on Anonymization Techniques (WP 216), 0829/14/EN.6.

[14] Article 29 Working Party (supra n. 13), 7/8.

[15] Information Commissioner's Office (November 2012), Anonymisation: managing data protection risk code of practice, 22, https://ico.org.uk/media/1061/anonymisation-code.pdf.

[16] STOA-Study (supra n. 5), 25 with further references.

[17] Jaccard/Tharin (supra n. 6), nos. 15 et seq.; for further details to the transactional data see Isler (supra n. 5), nos. 5 et seq. and STOA-Study (supra n. 5), 28 et seq.

[18] Federal Court, Case Logistep (2010), BGE 136 II 598; ECJ, Case C-70/10 Scarlet Extended (2011), EU:C:2011:771.

[19] ECJ, Case C-582/14 Breyer (2016), EU:C:2016:779.

[20] Jaccard/Tharin (supra n. 6), no. 18.

function with deletion of the key and tokenization.[21] A cryptographic hash is a mathematical function enabling to feed an input value by transforming it into an output value of fixed length. Technologically, the mere use of a hash function will not automatically transform personal data into anonymous data.[22]

[14] Pseudonymized data is based on the processing of personal data in such a way that an attribution to a specific data subject is no longer possible without the use of additional information. According to the EU Court of Justice someone cannot be considered as identifiable anymore if such an identification would be forbidden by law or not realizable in practice (disproportionate efforts in terms of time, costs, etc.).[23] The terminology used in the data protection context, however, does not fully coincide with the terminology of the blockchain community arguing that blockchains are pseudonymous rather than anonymous since the user attributes a pseudonym in the form of a public key.

[15] Anonymized (pseudonymized) data usually is encrypted data even if a formal definition is mostly missing in data protection laws. Perfectly anonymized (pseudonymized) data would in principle fall outside of the scope of data protection laws, if the criterion of irreversibility is fulfilled[24] and the representation of a near zero possibility to be linked to a person or entity can be given.[25]

3. Controller and Processor

[16] The proper designation of the data controller and the data processor is important since the allocation of regulatory tasks/obligations and particularly the corresponding responsibility and liability depend on the compliance or non-compliance with the legal provisions. Pursuant to Article 4(7) GDPR and Article 4(i) DPA, a controller is a natural or legal person determining the purposes and means of the processing of personal data. A controller can act alone or jointly with others; joint controllership is interpreted in a broad way in order to ensure the effective and complete protection of data subjects.[26]

[17] In the blockchain environment, the allocation of the controller and joint controller functions causes major difficulties and in principle requires distinguishing between private and public blockchains. The public blockchain is completely open, the private blockchain usually knows a centralizing function that attributes certain tasks to a specific provider. Therefore, the interme-

[21] For further details see STOA-Study (supra n. 5), 29/30; Jaccard/Tharin (supra n. 6), nos. 25 et seq.; Stengel/Aus der Au (supra n. 5), 442/43; Jörn Erbguth, Datenschutzkonforme Verwendung von Hashwerten auf der Blockchain, Multimedia und Recht 2019, 654 et seq.

[22] Hash functions with stronger privacy guarantees that may resist the «means reasonably likely to be used» test mentioned in Recital 26 GDPR have been developed (for example so-called «salted hashes» or «peppered hashes»); see also Christopher Millard, Cloud Computing Law, Oxford University Press, Oxford 2013, 178.

[23] See Art. 4(5) GDPR and Recital 29 GDPR; ECJ, C-582/14 Breyer (2016), EU:C:2016:779, nos. 46 et seq.

[24] See also Rolf H. Weber/Ulrike I. Heinrich, Anonymization, Springer, London et al. 2012, 1 et seq.

[25] See also Jaccard/Tharin (supra n. 6), nos. 27 et seq.

[26] Joint controllership is addressed in Art. 26(2) GDPR and (vaguely) in Art. 17 DPA; the respective main decision of the ECJ is the Case C-210/16 Wirtschaftsakademie Schleswig-Holstein (2018), EU:C:2018:388; from legal doctrine see Isler (supra n. 5), nos. 33 et seq.; STOA-Study (supra n. 5), 53/54.

diary of a transaction on a private blockchain is more likely to become a controller and be obliged to comply with data protection obligations.[27]

[18] Since the blockchain is based on distributed and decentralized databases, many actors can influence the determination of the processing means. The main target point is the application layer. The individual or a legal entity determining the processing of personal data at the application layer and executing a transaction can be seen as data controller. In private blockchains, mostly a specific legal entity determines the means and often also the purpose of the data processing; in such a situation, the Article 29 Working Party qualified the respective provider as data controller.[28]

[19] Due to the decentralized structure of a public blockchain, apart from infrastructure providers, also miners and even users can act as (at least joint) controllers of personal data relating to themselves. Technologically, the coders essentially determine how the rules of the particular blockchain network operate. In contrast, validating nodes usually do not process personal data and might insofar be less concerned about protection. For all these reasons, a generalizing assessment about the allocation of the controller function is hardly possible.[29]

[20] A specific problem consists in the fact that a controller is often not able to comply with the data privacy obligations since no sufficient control over the data on the blockchain is possible. In case of lack of control it is hardly feasible for the obliged addressee to implement the data protection measures required by data protection laws. So far, this aspect has not found any solution. The Article 29 Working Party has acknowledged that innovations in technology make it burdensome to determine controllership; it pleads for an allocation of responsibility in such a manner that compliance with data protection rules is ensured in the best possible way in practice. From the perspective of the data subject joint controllership can be an «escape» if several persons or legal entities are available to be targeted.[30]

[21] The processor of data on the blockchain is the natural or legal person or public body that processes personal data on behalf of the controller.[31] The Article 29 Working Party again exposed several elements that ought to be taken into account in order to determine whether someone is a processor, namely the level of instructions received from the data controller and the data controller's monitoring of the execution of the service.[32] Since the data processor only has a limited number of obligations, it is more likely that companies offering blockchain as a service comply with the data processor tasks based on a contractual relationship.

[27] See Jaccard/Tharin (supra n. 6), nos. 41 et seq.; Kelvin F. K. Low/Eliza Mik, Pause the Blockchain Legal Revolution, International and Comparative Law Quarterly 69/1 (2020), 135, 138–140.

[28] See Article 29 Working Party, Opinion 5/2009 on online social networking (WP 163), 01 189/09/EN, 5.

[29] For a detailed analysis with further references see STOA-Study (supra n. 5), 45–47; Jaccard/Tharin (supra n. 6), nos. 47 et seq.; a general technological overview is given by Gili Vidan/Vili Lehdonvirta, Mine the Gap: Bitcoin and the Maintenance of Trustlessness, New Media and Society 21/3 (2018), 42 et seq.

[30] Article 29 Working Party, Opinion 1/2010 on the concept of «controller» and «processor» (WP 169), 00264/10/EN, 21.

[31] Article 4(8) GDPR and Art. 4(j) DPA; see also Jaccard/Tharin (supra n. 6), no. 54 and STOA-Study (supra n. 5), 56/57.

[32] Article 29 Working Party (supra n. 30), 1.

4. Key Principles of Data Protection

[22] Modern data protection laws (such as the GDPR and the DPA) do not «invent» many new key principles but further develop and more clearly design already existing principles. Obviously, the jurisprudence related to the fundamental privacy rights stated in the European Convention of Human Rights of the Council of Europe (1950) as well as in the EU Treaty have to be taken into account by the legislators and do have an impact on the concretization of the data privacy principles.

4.1. Lawfulness and Transparency

[23] Pursuant to Article 5(1)(a) GDPR personal data shall be «processed lawfully, fairly and in a transparent manner in relation to the data subject» (similarly Article 5(1) und (2) DPA); the non-compliance with these central principles can cause a responsibility of the data controller. Various aspects are relevant in the context of the lawfulness and the transparency principle:

[24] (a) *Consent:* The processing of personal data is only legitimized if the concerned data subject has given the respective consent. Pursuant to Article 4(11) GDPR and Article 5(6) DPA the consent must be specific, informed, unambiguous and freely given. A particular form requirement does not exist, i.e. an electronic or an oral consent is sufficient (if it can be proven at a later stage) but silence or pre-ticked boxes are no valid forms of consent.[33] A possible line of arguing would be to state that by participating in a blockchain network an individual is impliedly giving his/her consent to the processing of the related data.

[25] In addition, the legislator can require that the consent must be given by way of an affirmative act and has to be explicit in respect of certain categories of data (Article 5(6) DPA). Furthermore, from a practical perspective in ongoing legal relations, the concerned data subject is free to withdraw his or her consent at any time (Article 7(3) GDPR). Even if particularities in the blockchain environment do insofar not exist the challenge in reality exists to find the correct addressee for such a withdrawal notification.

[26] (b) *Other Lawfulness Tests:* If the data subject does not or cannot give the consent or if the strict requirements of the consent are not met, the data processing is illegal if no alternative justification reason is available. Data protection laws usually encompass a number of lawfulness tests, for example the performance of a contract having been entered into by the data processor and the data subject, the compliance with a legal obligation, the protection of the vital interests of the data subject or another natural person, the carrying out of a task in the public interest or the exercise of official authority as well as the execution of general legitimate interests (detailed rules in Article 27 DPA).[34] In such cases, a balancing between the interests of the data controller and of the data subject must be conducted:[35] legitimate interests may be invoked if there is a «relevant and appropriate relationship between the data subject and the controller» (Recital 47 GDPR). The task to do a weighted balancing of interests usually leaves a broad room of manoeuvre or discretion.

[33] From the court practice see ECJ, Case 291/12 Michael Schwarz (2013), EU:C:2013:670, para. 32.

[34] See also STOA-Study (supra n. 5), 63.

[35] See for example ECJ Case C-13/16 Valsts policijas (2017), EU:C:2017:336; European Court, Case T 194-04 Bavarian Lager (2007), EU:T:2007:334.

[27] (c) *Transparency*: The principle of transparency is concretized in the information duties of the data controller. Articles 13/14 GDPR and Article 17 DPA list a large number of disclosure obligations which are to be met in order to justify the data processing. In particular, transparency regarding potential risks for the data subject as well as the easy access to the data are regulated.[36] In case of high risks, specific arrangements and governance obligations apply in order to protect the position of the data subject. In addition, the information has to be accurate throughout its life time.

4.2. Purpose Limitation

[28] An important principle of data protection laws is the purpose limitation of data processing. Pursuant to Article 5(1)(b) GDPR and Art. 5(3) DPA data shall be collected for specified and legitimate purposes and not further processed in a manner that is incompatible with those purposes. In respect of blockchain technologies, the question arises whether the further processing of data added to blocks after the execution of the transaction is compatible with the purpose limitation principle. In a given case, a substantive assessment of the compatibility of the initial purpose and the further processing must be made.[37] Also on the blockchain, personal data shall not be processed in a manner being incompatible with the legitimate purposes that have been communicated to the data subject at the beginning. According to the opinion of the Article 29 Working Party, a further processing is only legitimate to the extent that «a reasonable person in the data subject's position would expect his or her data to be used for based on the context of the collection».[38]

[29] The compliance with the purpose limitation principle causes challenges in the blockchain environment since the control over the block after the processing of a blockchain-based transaction is hardly possible anymore. Insofar, the technology restricts the full implementation of this principle. In order to overcome the respective problem, the anonymization of data offers a way out of the existing tensions.

4.3. Data Minimization and Storage Limitation

[30] (a) *Data Minimization:* Pursuant to Article 5(1)(c) GDPR data ought to be adequate, relevant and limited to what is necessary «in relation to the purposes for which they are processed» (similarly Article 5(3) DPA). Furthermore, Recital 39 GDPR specifies that personal data «should be processed only if the purpose of the processing could not reasonably be fulfilled by other means». As a consequence, an appropriate interpretation of the data minimization principle requires from the data processor or the data controller not to participate in the ever-growing data collection in databases. Instead of the quantity, the quality of the data must become important.[39]

[36] For details see Recitals 39 and 58 GDPR.

[37] Article 29 Working Party, Opinion 03/2013 on purpose limitation (WP 203), 00569/13/EN, 21–23.

[38] Article 29 Working Party (supra n. 37), 24.

[39] STOA-Study (supra n. 5), 68.

[31] The data minimization principle is crucial in the data privacy context and a cornerstone in the digital world, however, blockchain infrastructure does not add any further specific problems in its application.

[32] (b) *Storage Limitation:* Article 5(1)(e) GDPR and Article 5(4) DPA require from the data controller that no obsolete data is to be retained. In order to ensure that personal data is not kept longer than necessary, «time limits should be established by the controller for erasure or for a periodic review» (Recital 39 GDPR). In addition, every reasonable step must be taken to ensure that personal data being inaccurate is rectified or deleted (Article 5(5) DPA). This legal principle, however, does not answer the question under which circumstances certain data stored on the blockchain becomes obsolete. Furthermore, the technology does restrict the deletion of data on the blockchain.[40] Consequently, the storage limitation principle is not easy to comply with on the blockchain.

4.4. Data Subjects Rights

[33] Most data protection laws encompass a (large) number of rights vested in data subjects. With respect of these rights the blockchain infrastructure can cause problems, however, the respective tensions occur more severely in relation to some rights than in relation to other rights. Since the challenges in practice are lower due to less extensive technological restrictions (i) in case of the right to access (at least if the data controller is able to «control» the decentralized infrastructure), (ii) in case of the right to a restricted data processing (again to the extent «controllable») and (iii) in case of the right to object,[41] the focus is laid on those rights being particularly problematic in the blockchain environment hereinafter.

4.4.1. Right to Rectification

[34] Pursuant to Article 16 GDPR, the «data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her» (similarly Article 28(1) DPA). In case of private blockchains, compliance with such kind of requests can be done through an alteration of the relevant transaction records by re-hashing subsequent blocks. However, rectifying data on public blockchains is by far more difficult since the addressee of the rectification request might not be in a technical position to do the respective alteration. The challenges are also prevailing if all nodes, miners and users are considered to in fact qualify as data controllers.[42]

[35] The only remedy might often be the provision of a supplementary statement containing the contradiction of the concerned data subject as foreseen at the end of Article 16 GDPR and in

[40] For further details see Millard (supra n. 22), 182 and STOA-Study (supra n. 5), 69/70.

[41] For a more detailed discussion of these provisions see STOA-Study (supra n. 5), 71/72, 78/79 and 81/82.

[42] See also Jean Bacon/John David Michels/Christopher Millard/Jatinder Singh, Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledgers, Richmond Journal of Law & Technology 2018, 1 et seq.

Article 28(3) DPA. Such a statement can also be implemented on distributed ledgers, but it might not always be satisfactory for achieving compliance with the right to rectification.[43]

4.4.2. Right to Erasure / Right to be Forgotten

[36] One of the most intensively discussed amendments to the GDPR in comparison with the Data Protection Directive 95/46 is the explicitly stated right to erasure and (in broader terms) the right to be forgotten, the latter one based on the Google Spain decision of the European Court of Justice.[44] Pursuant to Article 17(1) GDPR the data subject shall have the right to «obtain from the controller the erasure of personal data concerning him or her without undue delay». This right to erasure is only limited to the extent that other fundamental rights are prevailing. The Article 29 Working Party has concretized the scope of data which should remain «forgotten» in the context of the informational self-determination.[45]

[37] The Swiss legislator has stated the (not contested) right to erasure in Article 28(2)(c) DPA. In contrast, the new DPA does not explicitly introduce a right to be forgotten since – according to the opinion of the Federal Council[46] – such a legal claim of an individual is already given based on the general personality right (Article 28 Swiss Civil Code). Looking at the available court practice this assessment appears to be correct, i.e. the EU and Swiss legal landscape are equivalent.

[38] Legal doctrine has pointed to the difficulty of applying the right to erasure to blockchains.[47] Technical factors play an important role but also the design governing the infrastructure. This assessment is particularly relevant since the precise meaning of the term «erasure» is often not clear. In view of the respective difficulties, regulators have tried to develop alternatives to the outright destruction of data, for example the anonymization or the «put beyond use» approach of data.[48] In a recent case the Court of Justice of the European Union appears to have indicated that erasure equals the destruction of personal data which is hardly achievable on the blockchain technology.[49] A possible alternative could be the destruction of the private key; other technical means might be based on anonymization or pseudonymization techniques.

[39] Furthermore, full erasure is only achieved if the personal data is removed from all of the nodes that participate in the network. Such a removal contradicts the technological principle of immutability governing the blockchain technology. Therefore, in order to achieve the desired objective, adequate techniques allowing a removal need to be developed. Since the technological means for the full erasure of data on the blockchain are not yet available, anonymization and

[43] See in this context the opinion of Attorney General Kokott in ECJ, Case C-434/16 Peter Nowak (2017), EU:C:2017:582, no. 35.

[44] ECJ, Case C-131/12 Google Spain (2014), EU:C:2014:317.

[45] Article 29 Working Party, Guidelines on the Implementation of the Court of Justice of the European Union Judgment on «Google Spain and Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González» C-131/12 (November 2014), 14/EN, WP 225.

[46] Botschaft (supra n. 4), 7077.

[47] Matthias Berberich/Malgorzata Steiner, Blockchain Technology and the GDPR – How to Reconcile Privacy on Distributed Ledgers?, European Data Protection Law Review 2 (2016), 422 et seq.

[48] STOA-Study (supra n. 5), 76/77; see also Jaccard/Tharin (supra n. 6), no. 59 and Stengel/Aus der Au (supra n. 5), 448.

[49] Case C-434/6 Peter Nowak (supra n. 43), no. 55.

pseudonymization measures are to be implemented as second-best solution in order to improve compliance with data protection laws.[50]

4.4.3. Right to Data Portability

[40] The right to data portability is one of the main innovations in the most recent amendments of data protection laws. The EU legislator provided for a relatively wide provision in Article 20 GDPR mainly targeting at the big social media enterprises. In Switzerland, the Federal Council was reluctant to introduce such a provision but in the parliamentary process the opinion prevailed that a right to data portability would be needed (now Article 25a DPA).

[41] Such a right to data portability can cause specific challenges in the context of blockchain technology. A first obstacle occurs if it is unclear which addressee of a request is able to control the concerned chain of data and to transmit the data to another provider since the addressee of the request must be in a position to find the block of data that needs to be migrated.[51]

[42] Secondly, the right to data portability is subject to interoperability among the various digital ledger technology solutions; moving a data block from Bitcoin to Ethereum may cause major technological problems. Therefore, the requirement of interoperability is often not fulfilled in practice and harmonized standards are not yet at the horizon. Possibly, data portability would mainly make sense where a blockchain has been used to secure data being an actual off-chain information about the user.

4.4.4. Right against Automated Data Processing

[43] The provisions of Article 22 GDPR and of Article 19 DPA on automated data processing are mainly relevant for smart contracts executed on the blockchain; smart contracts often make decisions by technological means without human involvement. A blockchain-based smart contract indeed may qualify as a decision. Consequently, the data subject's explicit consent must be obtained and the automated execution is necessary for the entering into or the performance of a contract between the data subject and the controller.[52] If the automated processing involves a high risk, a data protection impact assessment must be executed.

5. Blockchain as a Tool for Improving Data Privacy Objectives

5.1. Technological Developments

[44] Modern data protection laws do not only contain legal principles safeguarding data privacy; moreover, technological measures are foreseen that support the efforts to achieve this objective. These measures are equally relevant in the blockchain environment. The most prominent examples are technology-friendly data protection techniques such as data protection by design and by default. Therefore, Article 25 GDPR and Article 6(1) and (3) DPA impose an obligation on

[50] STOA-Study (supra n. 5), 77.

[51] For the interpretation of Art. 20 GDPR see Article 29 Working Party, Guidelines on the Right to Portability (2017), WP 16/EN, WP 242rev.01.

[52] For further details see Isler (supra n. 5), nos. 41 et seq. and Stengel/Aus der Au (supra n. 5), 448/49.

data controllers to implement the respective technical and organizational measures. Examples of such measures are pseudonymization and data minimization. The final aim consists in the realization of the constitutional fundamental rights framework.

[45] In order to combat the risks of non-compliance with fundamental rights in case of data processing and storage, controllers of data are obliged to conduct a so-called data protection impact assessment (Article 35 GDPR and Article 20 DPA). Such an analysis can be considered as special kind of risk assessment.[53] The technological measures need to be applied in a permanent way and they must be updated and modified if weaknesses are identified. The adopted internal policies for data protection that should also lead to an increased transparency and include functions which enable the data subjects to monitor the data processing can be subject to certification mechanisms.[54]

[46] In addition to the mentioned precautionary measures, technological developments might facilitate data privacy compliance, however, do also cause new challenges. As examples, the following blockchain-related mechanisms that improve compliance with data privacy principles in the new infrastructure environment are noteworthy:[55]

- *Zero knowledge proofs:* Such kind of proofs can be used to provide a binary true/false answer without providing access to the underlying data. The ledger merely reveals the execution of a transaction not the used public key and the transferred value.
- *Stealth addresses:* According to the Bitcoin White Paper,[56] stealth addresses make it possible to generate a one-kind transaction that relies on hashed one-time keys; nevertheless, a guarantee of privacy protection cannot be achieved.
- *Homomorphic encryption:* This technique is an advanced method of encryption enabling the computation of cypher texts; however, this solution could only serve as one element on a broader anonymization toolbox.
- *State channels and ring signatures:* State channels limit the sharing of information in two-parties smart contracts and allow disclosure of information to outside parties only in the event of a dispute. Ring signatures hide transactions by tying a single transaction to multiple private keys. So far, no legal certainty exists for developers wishing to handle public keys in a data privacy compliant manner.
- «*Addition of noise to data*»*:* This technical solution groups several transactions together so that from the outside it is impossible to discern the identity of the respective senders and recipients of a communication. But this solution should be combined with additional privacy mechanisms, for example with the removal of obvious attributes and quasi-identifiers.
- *Chameleon hashes and editable blockchain:* Engineers have created «editable» blockchains using chameleon hash functions to edit, remove or rewrite certain data. The stability of these measures depends on the surrounding governance arrangements.

[53] For further details see Thomas Janicki/David Saive, Privacy by Design in Blockchain-Netzwerken, Zeitschrift für Datenschutz 6 (2019), 251 et seq.

[54] See also Article 42 GDPR and Art. 12 DPA; further details are contained in the STOA-Study (supra n. 5), 98/99.

[55] The following list is based on STOA-Study (supra n. 5), 32 et seq. and Stengel/Aus der Au (supra n. 5), 450 et seq., both with further references.

[56] Bitcoin: A Peer-to-Peer Electronic Cash System, 2008 (https://bitcoin.org/bitcoin.pdf).

- *Storage limitations:* In contrast to the original blockchain idea of enabling to go back to the first block, storage limitation could provide an at least partial (but not a full) solution for data protection.
- *Pruning:* Technically, pruning should enable to remove data from the blockchain when it is no longer needed or wanted (in complying with the data minimization principle). Furthermore, the potential of secure multi-party computation as a future tool could be considered, equally as an indirection service in case of a third-party aggregation of many blockchain transactions enabling it to post them on the blockchain with its own public key.

[47] Even if the mentioned new technologies are not yet ripe, the developments appear to be promising. The data protection objectives might be better achieved by way of privacy supporting technologies instead of stricter normative rules.

5.2. Blockchain as Privacy-Enhancing Tool

[48] Notwithstanding the manifold difficulties to apply the data protection principles and obligations on the blockchain, it cannot be overlooked that the distributed ledger technologies also have the potential to be a tool of data governance and a tool that enables achieving compliance with the data privacy objectives.[57] This is the case since blockchain is a technology that enables data sharing without need of a central trusted intermediary and facilitates transactions by the use of smart contracts.

[49] In the context of the discussions about the creation of a digital market in Europe, voices have been raised that see blockchains as a potential solution capable of implementing data and market places for artificial intelligence development.[58] Such market places might be able to serve as intermediaries by creating contractual relations or data exchanges designed as closed platforms. If successful, such projects could present broader benefits to the data economy.

[50] The control over digitized data on blockchains eventually also increases the possibility of the data subjects to keep control over the personal data. The most often mentioned example is the development of tools regarding health data. The objective of such projects consists in giving the data subject the full decision-making power about the potential use of his or her data.[59]

[51] Similar mechanisms could also be suitable in other sectors. The objective would be to allow data sharing solutions depending on the decisions made by the data subject. Thereby, new forms of data management models can be implemented that would be able to ensure compliance with data access rights and to monitor the data controller’s observance of the general data protection principles.

[57] See STOA-Study (supra n. 5), 91 et seq.

[58] See European Parliament (27 November 2018), Report on Blockchain: a Forward-Looking Trade Policy (AB-0407/2018), para. 14.

[59] An example is the MIDATA cooperative in Switzerland, allowing the exchange of data between patients, medical doctors, hospitals and insurances (see https://www.midata.coop/).

5.3. Policy Options

[52] Participants being involved in the blockchain business or realizing government models might have to develop specific strategies that could be adopted in view of the privacy compliance requirements stated by data protection laws. Legal doctrine has discussed three common scenarios of how a data subject interacts with a blockchain, proposed a possible role assignment and developed applicable approaches for data minimization and compliance with fundamental rights:[60]

i. An individual interacts directly with a permissionless blockchain (for example exchange of cryptocurrencies): In such a situation no data controller can be identified, i.e. a person or entity being accountable for data privacy compliance can hardly be found. The only feasible approach for designers and engineers of permissionless blockchains consists in requiring from the users a consent for the data processing and in prohibiting the users from posting certain kinds of personal data.

ii. If applications using permissionless blockchains as backend (e.g. assets of Ethereum smart contracts) are used, the owner of the intermediary application can be qualified as data controller. In order to comply with the data protection rules any personal data must be hashed out to a server controlled by application developers. Currently, permissionless blockchains are organically evolving in order to minimize the amount of data stored and to avoid heavy processing.

iii. In case of permissioned blockchains a possible role assignment would be that all participants having access are considered to be joint data controllers. However, in such a case compliance with data protection principles would have to be realized by all participants.

[53] Apart from the mentioned scenarios, a stronger focus must be laid on regulatory guidance: The existing lack of legal certainty negatively influences the use of blockchain solutions. Therefore, further regulatory initiatives would be welcome. A possible approach could consist in the elaboration of a detailed questionnaire which is to be used as guidance in the decision-making processes (like a decision-tree).

[54] Finally, legal certainty could be improved by codes of conduct and certification mechanisms. Technology-neutral codes developed by industry associations (as foreseen in Article 10 DPA) are so far lacking and correspond to practical needs. The instrument of certification mechanisms is already foreseen in Article 42 GDPR and Article 12 DPA; it can be designed in a sufficiently broad way to be adapted to the specific technological requirements of blockchains. The certification may become part of the risk management and facilitate the initiation of related procedures.[61]

[60] See also STOA-Study (supra n. 5), 96 et seq. and Anja E. Dekhuijzen, Call for Action on the EDPB to Provide Guidance Concerning GDPR and Blockchain, Computer Law Review International 2019, 33 et seq.

[61] See STOA-Study (supra n. 5), 98/99.

6. Outlook

[55] In a nutshell, the following observations to the interplay of blockchain technology and privacy rights can be made:[62]

- Data protection laws apply to public and private blockchains almost without any geographical limitations if the used data fulfil the identifiability test allowing to «find» the concerned person. Furthermore, the basic technological term «processing» encompasses blockchain technology.
- Not only a private key as password, but also a public key must usually be considered as personal data if the identity of its holder can be determined by reconciliation with other data.
- Pseudonimization and anonymization techniques have the potential to become a solution to avoid triggering data protection obligations if a high technological standard is applied.
- The definition of the data controller or of a joint controller is very difficult in the blockchain environment. Apart from the sender of a transaction or the infrastructure provider, miners and/or users can also become joint data controllers under certain circumstances; validators of other nodes are less likely to fulfill the definitions contained in data protection laws.
- Certain data subject's rights can hardly be enforced under the current state of technology. In particular the right to rectification, the right to erasure/right to be forgotten and the right to data portability appear to be not easily feasible to put in practice on blockchains. Alternative technological solutions should be developed.
- Obligations related to privacy by design and privacy by default must be taken into account when creating a new blockchain; particularly if no joint data control of the full nodes is given, developers and designers of a blockchain could be exposed to liability.

[56] All over all, easy solutions for compliance with the data protection principles on the blockchain are not available. Moreover, assessments need to be made in view of the concrete circumstances on a case-to-case basis. The legal uncertainties can only be overcome in the long run if codes of conduct (and eventually certification regimes) give guidance on how the tensions between the digital ledger technologies and the data protection principles are to be reasonably solved. However, notwithstanding the existing challenges, blockchain also is suitable to be applied as privacy-enhancing tool if the technological design is appropriately developed.

Prof. Dr. Rolf H. Weber, em. Professor at the University of Zurich, Faculty of Law, Zurich, Switzerland, and practicing attorney-at-law, Bratschi AG, Zurich; rolf.weber@rwi.uzh.ch.

Internet sources have last been checked on 1 June 2020.

[62] See also Jaccard/Tharin (supra n. 6), no. 62.