Data Protection Issues for Smart Contracts

W. Gregory Voss

4

Data Protection Issues for Smart Contracts

W GREGORY VOSS

I. Introduction

Smart contracts offer promise for facilitating and streamlining transactions in many areas of business and government. However, they also may be subject to the provisions of relevant data protection laws, if personal data is processed. The term 'data protection' is a European one, which generally is considered a broader concept than 'privacy'. Data protection includes requirements regarding data security, the provision of rights to the individuals to whom the data relate (data subjects) and data processing. In this respect it is a broader concept than the American one of 'information privacy', and sometimes 'data privacy' is used as a compromise term for comparative law purposes to serve as a synonym for data protection.[1] However, data protection is based on transparency, in that those processing data are to do so in a manner that is 'open, fair, appropriate and secure' whereas privacy generally seeks opacity for private information.[2]

Data protection has come to be exemplified by EU legislation, which has helped shape legislation in other jurisdictions around the globe.[3] However, models other than the EU individual rights one exist, such as the US laissez-faire/self-regulation model and the Chinese model centred around national interest.[4] Nonetheless, even in the US current and proposed state data privacy laws are being influenced by EU legislation.[5] This chapter, however, will focus on EU legislation faced with the data protection legal issues that arise through the use of what are called 'smart

[1] WG Voss, 'Obstacles to the Harmonization of Data Privacy Law in Context' (2019) *University of Illinois Journal of Law, Technology & Policy* 405, 408–09.

[2] R Brownsword and M Goodwin, *Law and the Technologies of the Twenty-First Century: Text and Materials* (Cambridge, Cambridge University Press 2012) 308.

[3] Voss, 'Obstacles to the Harmonization' (2019) 411.

[4] WG Voss, 'Cross-Border Data Flows, the GDPR, and Data Governance' (2020) 29 *Washington International Law Journal* 485, 489–93.

[5] Voss (n 1) 498–501.

contracts' – computer processing that executes autonomously.[6] Smart contracts use the blockchain or distributed ledger technology system whereby transactions are stored on various computers (referred to as 'nodes') of a blockchain network, using a consensus algorithm.[7] They also are executed independently of the control of any one actor, according to a computer program (or code).[8] However, the decentralised system of smart contracts using blockchain technology contrasts with the classical centralised system of data collection and storage that the legislators had in mind when they crafted EU legislation,[9] which has raised certain issues that this chapter will detail. Indeed, that legislation was designed and written prior to blockchain technology becoming widely known.[10]

Certain observers have spoken of 'the clash between the GDPR and blockchain technology',[11] referring to the common abbreviation used for the current EU data protection legislation, or of their being 'incompatibile, the digital equivalent of oil and water'.[12] De Filippi and Wright remark that, 'Without strong privacy protections, smart contracts likely will prove unsuitable for legal agreements where confidentiality is crucial.'[13] In this discussion, the reader should keep in mind the distinction between public blockchains, which 'allow anyone to participate in the consensus process, the process for determining which transactions and which blocks are added to the chain',[14] and private blockchains, where participants are known and are bound by terms and conditions.[15] Most legal issues (including privacy ones) arise in connection with public blockchains.[16]

After this introduction, section II briefly explains the GDPR. Section III discusses personal data in smart contracts and section IV delves into details about data protection accountability in the context of smart contracts. Section V investigates data subject rights in the context of smart contracts, section VI covers integrity and confidentiality in the context of the blockchain, and section VII highlights two additional data protection principles relevant in the context of

[6] P De Filippi and A Wright, *Blockchain and the Law: The Rule of Code* (Cambridge, Massachusetts, Harvard University Press 2018) 2.

[7] M Finck, 'Blockchains and Data Protection in the European Union' (2018) 4 *European Data Protection Law Review* 17.

[8] M Finck, 'Smart contracts as a form of solely automated processing under the GDPR' (2019) 9 *International Data Privacy Law* 79.

[9] Finck, 'Blockchains' (2018) 17.

[10] P Van Eecke and AG Haie, 'Blockchain and the GDPR: The EU Blockchain Observatory Report' (2018) 4 *European Data Protection Law Review* 531.

[11] D Meyer, 'Blockchain technology is on a collision course with EU privacy law' *iapp* (27 February 2018), available at iapp.org/news/a/blockchain-technology-is-on-a-collision-course-with-eu-privacy-law.

[12] G Bailey, 'Blockchain And EU Privacy Laws: A Three-Step Guide To Compliance' *Forbes* (22 February 2019), available at www.forbes.com/sites/georgebailey1/2019/02/22/blockchain-and-eu-privacy-laws-a-three-step-guide-to-compliance.

[13] De Filippi and A Wright, *Blockchain and the Law: The Rule of Code* (2018) 83.

[14] E Mik, 'Blockchains: A Technology for Decentralized Marketplaces' in LA DiMatteo, M Cannarsa and C Poncibò (eds), *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms* (Cambridge, Cambridge University Press, 2020) 163.

[15] Mik, 'Blockchains' (2020) 164.

[16] ibid 165.

the blockchain – purpose limitation and data minimisation. Finally, section VIII concludes with the idea that although smart contracts and data protection legislation are not completely incompatible, a good undertstanding of the latter is necessary in order for smart contracts not to violate the legislation.

II. The EU Data Protection Legislative Framework

The current EU data protection legislation is the General Data Protection Regulation (GDPR),[17] which was adopted in 2016, but became applicable on 25 May 2018.[18] The GDPR applies to the processing of the personal data[19] of an individual in the EU when the GDPR's material and territorial scope requirements are met.[20] The concept of processing is a very broad one in the GDPR:

> [A]ny 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.[21]

Several of these actions would be performed when personal data are included in smart contracts, which involve adaptation and structuring into computer code, dissemination to the various nodes on the blockchain, storage there, disclosure by transmission, use, and so on.

The GDPR has extraterritorial scope and extends to the processing of personal data of those in the EU by data controllers[22] even when they do not have an establishment there, if the processing is related to 'the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or the monitoring of their behaviour as far as their behaviour takes place within the Union'.[23] This is likely to be easy to determine, at least insofar as a permissionless network is concerned, 'since anybody can use an open/permissionless platform, operators of such platforms may be deemed to offer services to data subjects in the EU'.[24] Thus, 'European data protection rules are likely to

[17] Council Regulation 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) (EU) 2016/679 [2016] OJ L 119/1.

[18] Article 99 of the GDPR.

[19] For a definition of this term, see text to n 36.

[20] Articles 2–3 of the GDPR.

[21] Article 4(2) of the GDPR.

[22] For a definition of this term, see text to n 60.

[23] Article 3(2) of the GDPR.

[24] J Bacon, JD Michels, C Millard and J Singh, 'Blockchain Demystified' (2017) Queen Mary University of London, School of Law, Legal Studies Research Paper No. 268/2017, 39, available at ssrn.com/abstract=3091218.

apply to many blockchain-based transactions that have little or no connection to Europe'.[25] While the GDPR has a dual objective, protecting 'fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data'[26] and ensuring that the 'free movement of personal data within the Union … be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data',[27] it also establishes a limitation on the transfer of personal data to a county outside of the EU to those countries for which 'the Commission has decided that the third country … ensures an adequate level of protection'.[28]

Furthermore, the GDPR provides significant rights to data subjects,[29] and introduces data protection compliance mechanisms such as data protection impact assessments and data protection officers,[30] in addition to data processing registers for most controllers, other than certain SMEs.[31] The GDPR contains various data breach notification requirements,[32] and gives reinforced powers to supervisory authorities,[33] including the power to 'impose a temporary or definitive limitation including a ban on processing',[34] and to levy administrative fines going up to a maximum of the higher of 20 million euros or four per cent of total worldwide annual turnover of the proceding financial year, in the case of an undertaking.[35]

The next section discusses the GDPR concept of personal data in the context of smart contracts.

III. Personal Data in Smart Contracts

This section begins by setting out the definition of 'personal data' (section III.A), then details data not subject to personal data protection (section III.B), developing this through a discussion of anonymous information, anonymised information, and pseudonymisation (section III.C), prior to applying this to the blockchain context (section III.D).

[25] W Maxwell and J Salmon, *A guide to block chain and data protection* (London, Hogan Lovells, 2017) 11.
[26] Article 1(2) of the GDPR.
[27] Article 1(3) of the GDPR.
[28] Article 45(1) of the GDPR.
[29] See text to n 80.
[30] WG Voss, 'Internal Compliance Mechanisms for Firms in the EU General Data Protection Regulation' (2018) 50 *Revue juridique Thémis de l'Université de Montréal* 801–14.
[31] Article 30 of the GDPR.
[32] Articles 33–34 of the GDPR.
[33] Article 58 of the of the GDPR.
[34] Article 58(2)(f) of the GDPR.
[35] Article 83(5) of the GDPR.

A. Definition of 'Personal Data'

The GDPR employs a broad concept of personal data. As the processing of personal data triggers the application of the GDPR this is important. Personal data means:

> Any information relating to an identified or identifiable natural person ('data subect'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[36]

As a practical matter, this definition extends greatly, because of the fact that the data subject need not specifically be identified by the data; being identifiable suffices. The definition specifically refers to identification numbers and online identifiers, but other examples of what might be considered personal data include not only names and addresses, names used in connection with a telephone number, biometric data, video images of individuals, but also health information, working time information, and in many cases, IP addresses.[37]

B. Data not Subject to Personal Data Protection

However, as indicated in its recitals, and as may be gathered from the definition of 'personal data', which refers solely to information relating to a natural person, the data of companies and other legal persons do not benefit from protection under the GDPR: 'This Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person.'[38] In addition, the personal data of those who are deceased are not covered by the GDPR, although EU Member States are given the leeway to legislate in this regard.[39] Furthermore, properly anonymised data are not considered personal data and thus fall out of the scope of the GDPR, as well:

> The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.[40]

[36] Article 4(1) of the GDPR.

[37] WG Voss and KA Houser, 'Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies' (2019) 56 *American Business Law Journal* 287, 316–20.

[38] Recital 14 of the GDPR.

[39] Recital 27 of the GDPR.

[40] Recital 26 of the GDPR.

Anonymisation is a procedure that, when properly carried out, allows various new technologies to be used in compliance with the GDPR. Thus, the next subsection details it further.

C. Anonymous Information, Anonymised Information and Pseudonymisation

The GDPR refers to anonymous information as being 'information which does not relate to an identified or identifiable natural person' and anonymised information as 'personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable'.[41] However, further guidance, indicating a risk-based approach, has been adopted:

> To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.[42]

Time and cost, then, are taken into consideration when evaluating whether or not anonymisation is successful and will be considered as such under the GDPR. If so, the data are no longer considered personal data. Advisory guidance indicates that anonymisation must be 'irreversible'.[43] Furthermore, pseudonymised data do not fit within the definition of anonymised information, as the relevant natural person could be identified by using additional information.[44] As a result, they are still treated as personal data subject to the requirements of the GDPR, although pseudonymisation may be used as an element of data security.[45]

D. Application in the Blockchain Context

In the blockchain context, transactional data stored in blocks and public keys may potentially be classified as personal data.[46] Encryption does not remove transactional data from the category of personal data, as it is still possible to access the data using the relevant encryption keys.[47] Furthermore, experts can probably still link the data to an individual, through adequate effort.[48] Likewise, transactional data

[41] Recital 26 of the GDPR.
[42] Recital 26 of the GDPR.
[43] Article 29 Data Protection Working Party, 'Opinion 05/2014 on Anonymisation Techiques' (2014) 5, available at www.pdpjournals.com/docs/88197.pdf.
[44] Recital 26 of the GDPR.
[45] Recital 28 of the GDPR.
[46] Finck (n 7) 22.
[47] ibid.
[48] Maxwell and Salmon, *A guide to block chain and data protection* (2017) 7.

that has gone through a hashing process is still considered personal data, as the hashing is considered a pseudonymisation technique.[49] Hashes are 'mathematical derivations of data that, if properly implemented, cannot be reverse-engineered to expose the data that's being represented – but you *can* use them to verify the underlying data'.[50]

One solution to these issues is to store all personal data off the blockchain, although developers need to be careful not to thwart this by use of metadata that may reveal personal data.[51] For example, 'with respect to metadata, if the platform's users are natural persons, the sender's and recipient's addresses will almost always qualify as personal data'.[52] Another solution would be to restrict use to the business-to-business (B2B) context, as 'if a platform's users are all legal persons (such as businesses) the platform could be designed such that the metadata does not contain information related to natural persons'.[53]

Public keys are likely to be considered pseudononymous data, as connecting them with additional information will permit identification, and these keys cannot be moved 'off-chain',[54] and as such they continue to be considered personal data. The presence of personal data, and their processing, trigger the application of the GDPR, if that legislative instrument's material and territorial scope requirements are met.

Next, this chapter goes into detail about data protection accountability in the context of smart contract.

IV. Accountability in Smart Contracts

This section begins by setting out the concept of accountability (section IV.A), then sets out the definitions of controller and joint controller (section IV.B), prior to discussing guidance from the CNIL and public permissionless blockchains (section IV.C). It continues by detailing the contrasting position of controllers in permissioned blockchains (section IV.D), and concludes with recommendations from the CNIL (section IV.E).

A. The Concept of Accountability

Accountability in the GDPR relates to the concept that someone must be responsible for data protection law compliance. Generally, it is the controller that has

[49] Finck (n 7) 23.
[50] Meyer, 'Blockchain technology' (2018).
[51] ibid.
[52] Bacon, Michels, Millard and Singh, 'Blockchain Demystified' (2017) 40.
[53] ibid 41.
[54] ibid 24–25.

the main responsibility under the GDPR, and they are considered 'key actors in the operationalisation of data protection law as they are the primary bearers of the obligations set by such law toward data subjects'.[55] The GDPR provides that, 'the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed accordance with this Regulation. Those measures shall be reviewed and updated where necessary'.[56] This accountability does not limit itself to the literal content of the GDPR, but may involve an 'ethical assessment'[57] and have as a goal improving corporate data governance.[58] A first determination that should be made is that of the party who is the controller, that is, the party to whom a data subject would turn 'to find out from the controller if his or her data is being processed, and if so, for what purpose, who the data is being shared with, and so on', using their right to access,[59] or the party that a supervisory authority would hold responsible in the event of data protection law violations.

B. Definition of 'Controller' and 'Joint Controller'

The GDPR defines a controller 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.[60]

However, the GDPR has also added specific reference to joint controllers, meaning that more than one person may have the responsibility for GDPR compliance in the processing of certain personal data. The term 'joint controller' is defined not in the definitions article of the GDPR, but in a specific article devoted to this category of actor – GDPR Article 26. Joint controllers exist, 'where two or more controllers jointly determine the purposes and means of processing', in which case the joint cotrollers are to determine together their respective responsibilities for data protection compliance 'in a transparent manner',[61] which typically means by written contract. Although 'there is no explicit obligation for the arrangement to

[55] LA Bygrave and L Tosoni, 'Article 4(7). Controller' in C Kuner, LA Bygrave and C Docksey (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford, Oxford University Press, 2020) 146.

[56] Article 24(1) of the GDPR.

[57] Voss, 'Internal Compliance Mechanisms' (2018) 819.

[58] D Le Métayer, 'Whom to Trust? Using Technology to Enforce Privacy' in D Wright and P De Hert (eds), *Enforcing Privacy: Regulatory, Legal and Technological Approaches* (Cham, Springer, 2016) 427.

[59] T Lyons, L Courcelas and K Timsit, 'Blockchain and the GDPR' (2018) 25, available at www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf.

[60] Article 4(7) of the GDPR (emphasis added).

[61] Article 26(1) of the GDPR.

be recorded in writing', in connection with transparency requirements vis-à-vis the data subject, it is implied that at the least a summary of the arrangements between the joint controllers should be in writing.[62] The GDPR provides that where joint controllers, or joint processors, or a controller and a processor involved in the same processing, and responsible for damage caused by it, 'each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject'.[63] Effectively, by a system of joint and several liability this shifts the burden of sorting out the relative responsibilities of the joint controllers to them, through their arrangements, including any provisions as to compensation by one joint controller to the other when it pays out the entire damage compensation.[64]

C. Guidance from the CNIL and Public Permissionless Blockchains

The French supervisory authority, the *Commission nationale informatique et libertés* (CNIL) addresses the identification of data controllers in the blockchain in guidance issued in 2018, while acknowledging that the GDPR was designed for a world where data are managed centrally, unlike the decentralised blockchain model.[65] The CNIL advised that participants in a blockchain may be considered controllers if they have the right to write on the blockchain and send the data on to the miners for validation, as they define the objectives of the data processing and its means, including the data format and use of the blockchain itself.[66] The importance of this fact is that, if each node on the smart contract blockchain is treated as a controller, then they all need to comply with the GDPR.[67] Finck acknowledges that it is likely, in the case of a public permissionless blockchain, that each node is an independent controller (and not a joint controller) as they are 'not subect to external instructions, autonomously decide whether to join the chain, and pursue their own objectives' and do not jointly determine processing purposes and means with other nodes, and they shape the system by their individual behaviour.[68] This causes problems, as it is difficult to determine nodes' number,

[62] C Millard and D Kamarinou, 'Article 26. Joint controllers' in C Kuner, LA Bygrave and C Docksey (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford, Oxford University Press, 2020) 587.

[63] Article 82(4) of the GDPR.

[64] Millard and Kamarinou, 'Article 26. Joint controllers' (2020) 583.

[65] CNIL, 'Blockchain: Solutions for a responsible use of the blockchain in the context of personal data' (2018) 1, available at www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf.

[66] ibid 1.

[67] LA DiMatteo, M Cannarsa and C Poncibò, 'Smart Contracts and Contract Law' in LA DiMatteo, M Cannarsa and C Poncibò (eds), *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms* (Cambridge, Cambridge University Press, 2020) 15.

[68] Finck (n 7) 26.

identity and location, and nodes only see the encrypted or hashed version of the data and cannot change them, thereby rendering nodes incapable of responding to data protection tasks.[69]

D. Controllers in Permissioned Blockchains

Certain authors assert that in private and consortium blockchain platforms, otherwise known as 'permissioned blockchains' operated by one organisation or a consortium, it may be feasible to identify a central controller; although in a public blockchain, every node may qualify as a controller.[70] Lokke Moerel contends that a form of self-regulation may provide the answer, at least in the case of permissioned blockchains, stating that already 'private and consortium platforms implement membership rules, determining which parties have read or read/write authorization' and also determining who is the responsible entity.[71] Additionally, much as we have seen the rise of platforms as key intermediaries in the Internet infrastructure, Moerel sees the possibility of the rise of new intermediaries in permissioned private and consortium platforms, thus solving the mystery of who is the controller.[72] Furthermore, according to the CNIL, miners are not considered controllers,[73] and an individual using smart contracts strictly for a personal or household activity would also not be considered a controller,[74] as this would fall within an exception to the material scope of the GDPR.[75]

E. Recommendations from the CNIL

The CNIL recommends that the parties carrying out the processing activities with a common purpose identify the controller, perhaps by creating a legal person to play this role, or by appointing one party to make decisions for the group and designating it as the controller.[76] It also comments that the algorithm developer may be a mere supplier or, if it participates in the processing, may be considered a processor or a controller, depending on whether or not it determines the purposes of the processing.[77] A smart contract developer processing personal data on a controller's behalf would be considered a processor, and miners may also be

[69] ibid 26.

[70] L Moerel, 'Blockchain and Data Protection' in LA DiMatteo, M Cannarsa and C Poncibò (eds), *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms* (Cambridge, Cambridge University Press, 2020) 215–16.

[71] ibid 222.

[72] ibid 221.

[73] CNIL, 'Blockchain' (2018) 2.

[74] ibid.

[75] Article 2(2)(c) of the GDPR.

[76] The CNIL refers to French forms of legal persons here – associations and economic interest groups. CNIL (n 65) 2.

[77] ibid 2.

considered processors, thus the CNIL recommends that the miners enter into a contract with the participant, which specifies their respective obligations, pursuant to the provisions of Article 28 of the GDPR.[78] This chapter now turns to the main data subject rights that cause difficulties in connection with smart contracts using the blockchain's distributed ledger technology.

V. Data Subject Rights in the Context of Smart Contracts

This section begins with an introduction on data subect rights (section V.A), prior to discussing two important rights in the context of the compatibility of smart contracts with EU data protection law – the right to rectification and the right to erasure ('right to be forgotten') (section V.B), and an additional right – that not to be subject to a decision based solely on automated processing (section V.C).

A. Introduction on Data Subject Rights

One difficulty that arises in data protection compliance when smart contracts are used is the exercise of data subject rights. This is because of the immutability of smart contracts – by default the code of the smart contracts cannot be changed,[79] while some of the data subject rights involve erasing or changing the data. Data subjects rights, which were expanded in the EU with the adoption of the GDPR, now include a right of access, rights to rectification, to erasure ('right to be forgotten'), to restriction of processing, to data portability, to object to processing, and the right not to be subject to automatic decision-making or profiling (with exceptions).[80] Former European Parliament Member Jan Philipp Albrecht, the rapporteur of the GDPR, commented that:

> Certain technologies will not be compatible with the GDPR if they don't provide for [the exercising of data subject's rights] based on their architectural design … This does not mean that blockchain technology in general has to adapt to the GDPR, it just means that it probably cannot be used for the processing of personal data.[81]

The CNIL considers that the related data subject information rights are not a problem, and the exercise of the right of access and the right to data portability are compatible with the blockchain.[82] However the right to rectification and the right to erasure ('right to be forgotten') deserve more attention, and the right not to be

[78] ibid 3.
[79] DiMatteo, Cannarsa and Poncibò, 'Smart Contracts and Contract Law' (2020) 4.
[80] Voss, 'Obstacles' (2019) 421.
[81] Meyer (n 11).
[82] CNIL (n 65) 8.

subject to a decision based solely on automated processing merits 'careful consideration in advance.'[83]

B. Right to Rectification and Right to Erasure ('Right to be Forgotten')

Specifically, the use of smart contracts in connection with personal data poses problems for GDPR compliance in connection with the 'right to rectification' and the 'right to erasure' ('right to be forgotten') due to the smart contracts' immutability.[84] This section begins with a discussion of the right to rectification (section V.B.i), and continues with a somewhat more developed discussion on the related right to erasure ('right to be forgotten') (section V.B.ii).

i. Right to Rectification

The right to rectification is set out in Article 16 of the GDPR:

> The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete person data completed, including by means of providing a supplementary statement.[85]

The right to rectification relates to the data quality data protection principle, specifically providing that personal data shall be 'accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay'.[86] It is a longstanding principle, which virtually mirrors the language of prior EU law,[87] and reflects one of the 'fair information principles' distilled in a 1973 report commissioned by the US Department of Health, Education and Welfare.[88] However it does not sit well with the blockchain, as it is 'technically impossible' to grant a right to rectification 'when cleartext or hashed data is recorded on a blockchain', thus the CNIL strongly recommends 'not to register personal data in cleartext on a blockchain, and to use one of the cryptographic solutions' it discusses.[89] Furthermore the updated data would need to be entered in a new block.[90]

[83] CNIL (n 65) 8–9.
[84] Moerel, 'Blockchain and Data Protection' (2020) 227.
[85] Article 16 of the GDPR.
[86] Article 5(1)(d) of the GDPR.
[87] Article 6(1)(d) of the Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data 95/46/EC [1995] OJ L281/31 Art 6(1)(d).
[88] G González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Cham, Springer, 2014) 34.
[89] CNIL (n 65) 9.
[90] ibid 9.

ii. Right to Erasure (the 'Right to be Forgotten')

The main provision of the right to erasure ('right to be forgotten'), a related right described as 'more of a detailed elaboration of the already existing right of erasure' than a novelty,[91] is contained in Article 17(1) of the 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 and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:
>
> (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
> (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
> (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
> (d) the personal data have been unlawfully processed;
> (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
> (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).[92]

Where a request for exercise of the right to erasure is made an analysis of the basis for the request must be made, to see if it fits within one of the grounds listed above. If processing of the data is required for contract performance, where the data subject is a party to the contract, then the processing is lawful[93] and likely none of the cases for erasure listed in Article 17(1) would apply. This is consistent with a statement by the Commission during the legislative process prior to adoption of the GDPR, 'personal data may be kept for as long as it is needed to carry out a contract or to meet a legal obligation (for example when citizens have a loan contract with their bank). In short, the right to be forgotten is not absolute'.[94] However, an analysis has to be done to ensure that the processing truly is necessary for contract performance, 'an objective assessment that must be conducted prior to the commencement of the processing'.[95] Futhermore, additional exceptions to this right of erasure apply, such as where the data are necessary for the exercise or

[91] H Kranenborg, 'Article 17. Right to erasure ("right to be forgotten")' in C Kuner, LA Bygrave and C Docksey (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford, Oxford University Press, 2020) 477.

[92] Article 17(1) of the GDPR.

[93] Article 6(b) of the GDPR.

[94] European Commission, 'Data Protection Day 2014: Full Speed on EU Data Protection Reform' MEMO 14–60 (27 January 2014), available at ec.europa.eu/commission/presscorner/detail/en/MEMO_14_60.

[95] W Kotschy, 'Article 6. Lawfulness of processing' in C Kuner, LA Bygrave and C Docksey (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford, Oxford University Press, 2020) 331.

defence of legal claims.[96] Nonetheless, where the right does apply and when it is exercised by the data subject, the controller must erase the data and, where it has made the data public, inform controllers processing the data 'that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data'.[97]

While the 'right to be forgotten' is not absolute and a balancing test between data protection and other fundamental rights may need to be applied, a private transaction has less chance of prevailing over data protection than, say, a public interest register such as the Italian public company register in the *Manni* case (decided under EU law prior to the GDPR), or for landownership or trademark ownership ledgers.[98] Thus, where personal data is stored on the blockchain network of any particular smart contract, and an exception does not apply, the right to erasure is problematical as it is almost impossible to delete the data once they are on the blockchain.[99]

The right to erasure creates difficulties in the context of smart contracts using blockchain technology, as blockchain networks are built to create trust by making it impossible to delete or modify transaction records without breaking the chain. 'The whole point of such a blockchain is to ensure that transactions, including the parties to them, are never forgotten in order to enable decentralised trust'.[100] Furthermore, restricting the use of smart contracts to private, permissioned blockchain networks does not remove the problem 'unless that network is designed in a way that each and every piece of data is readable by only the parties that absolutely need to, and can be rectified or erased at the request of the data subject'.[101] While 'it is technically impossible to grant the request for erasure made by a data subject when data is registered on a blockchain', the CNIL has opened the door a bit to exploring technical solutions:

> However, when the data recorded on the blockchain is a commitment, a hash generated by a keyed-hash function or a ciphertext obtained through 'state of the art' algorithms and keys, the data controller can make the data practically inaccessible, and therefore move closer to the effects of data erasure.[102]

Nonetheless, the CNIL reminds the reader that 'these solutions do not, strictly speaking, result in an erasure of the data, insofar as the data would still exist in the blockchain'.[103] Maxwell and Salmon comment that the concept of 'erasure' is still

[96] Article 17(3) of the GDPR.
[97] Article 17(2) of the GDPR.
[98] Moerel (n 70) 228.
[99] R de Caria, 'Definitions of Smart Contracts: Between Law and Code' in LA DiMatteo, M Cannarsa and C Poncibò (eds), *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms* (Cambrdige, Cambridge University Press, 2020) 35.
[100] Lyons, Courselas and Timsit, 'Blockchain and the GDPR' (2018) 25.
[101] ibid 25.
[102] CNIL (n 65) 8.
[103] ibid 9.

open; some supervisory authorities admit that irreversible encryption satisfies the requirement.[104] Furthermore, smart contract mechanisms governing access rights 'can be used to revoke all access rights, thereby making the content invisible to others, albeit not erased'.[105] Certain observers look forward to supervisory authorities issuing guidance evidencing a pragmatic approach in the future.[106]

C. Right not to be Subject to a Decision Based Solely on Automated Processing

Michèle Finck argues that a smart contract 'will only in some circumstances be connected to a legal contract' but always will constitute automated data processing.[107] Thus, by a few keystrokes she cautions that the requisite contract legitimate basis for processing personal data may not exist in many smart contracts and she also holds up the spectre of an additional data subject right – that 'not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her'.[108]

In that case, where the contract legitimate basis does not exist, a potential exception to the prohibition on automated individual decision-making – where 'necessary for entering into, or perfomance of, a contract between the data subject and a data controller'[109] – would also not be available. There would also be significant difficulties using this exception when public and permissionless blockchains 'that can be read and used by anyone are used to execute the smart contract', as this does not jibe with the requirement of a contract between the data subject and the data controller.[110] Furthermore, an exception based on the explicit consent of the data subject[111] would be difficult to use in the context of the immutable blockchain, as the data subject would have a right to withdraw consent at any time, and 'it may be difficult for a data subject to put an end to the data processing in revoking consent' where personal data should then be deleted by the controller.[112] Moreover, withdrawing consent provides a ground for the exercise of the right to erasure.

There are other difficulties related to the prohibition on decisions based solely on automated processing such as complying with the right to human intervention,

[104] Maxwell and Salmon (n 25) 15.
[105] ibid 15.
[106] Van Eecke and AG Haie, 'Blockchain and the GDPR' (2018) 534.
[107] Finck (n 7) 79.
[108] Article 22(1) of the GDPR.
[109] Article 22(2)(a) of the GDPR.
[110] Finck (n 7) 85.
[111] Article 22(2)(c) of the GDPR.
[112] Finck (n 7) 87.

which Finck sees as an unavoidable requirement.[113] In addition, under certain conditions, the use of automated processing may give rise to the requirement that a data protection impact assessment be carried out,[114] as the the blockchain infrastructure used by smart contracts 'involves a high risk from a data protection perspective'.[115]

This chapter now turns to the GDPR's handling of security risks, under a data protection concept that is now referred to as 'integrity and confidentiality'.

VI. Integrity and Confidentiality in Smart Contracts

This section begins by introducing the concept of integrity and confidentiality under the GDPR (section VI.A), prior to developing this subject in the context of the blockchain and smart contracts (section VI.B).

A. Introduction on Integrity and Confidentiality under the GDPR

Security is an important element of EU data protection law, which the GDPR categorises under the 'integrity and confidentiality data protection principle', providing that personal data shall be 'processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures'.[116]

The GDPR also takes a risk-based approach in providing that:

> Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.[117]

Various tools may be used to improve security of personal data, such as pseudonymisation and encryption.[118] Furthermore, controllers have responsibility for ensuring the selection of processors that offer 'sufficient guarantees to implement appropriate technical and organisational measures in such a manner

[113] ibid 87.
[114] ibid 90.
[115] ibid 91.
[116] Article 5(1)(f) of the GDPR.
[117] Article 32(1) of the GDPR.
[118] Article 32(1)(a) of the GDPR.

that processing will meet the requirements' of the GDPR and 'ensure the protection of the rights of the data subject', including security requirements.[119]

B. Integrity and Confidentiality in the Context of the Blockchain and Smart Contracts

Integrity and confidentiality (security) is a data protection principle that involves issues in connection with smart contracts using blockchain technology. Not only are there risks of bugs in the computer code, but there are also real dangers of hacking, as evidenced by a case involving the hacking of the Etherum blockchain.[120] In that case, a distributed crowdfunding system, the DAO, was created with corporate governance and operations conducted through the use of smart contracts.[121] Shortly after launching, a hacker profited from a bug in the code to 'siphon off' over $60 million in cybercurrency contributed by users. There was 'no legal or technical way' to recover the funds as things stood, so the leaders of the project had to convince a majority of the nodes to implement a 'hard fork' splitting the blockchain into two paths, which allowed recovery of the funds, but killed off the project.[122] This concept of a 'fork' is explained by ENISA, the European Union Agency for Cybersecurity:

> One of the key aspects of a distributed ledger is that the data held within it, is considered valid because all parties agree to a single 'true' version. In the event that existing participants in a Blockchain decide to include data in a non-compliant manner with established protocols, an event named a fork occurs.
>
> Forks result in a split of the ledger and the consequent creation of two groups, each validating their own version of the ledger. In order for participants to be able to continue to interact with each other, they are required to follow the same fork of the ledger.[123]

However, while the use of a fork is relatively simple on a private blockchain, is is 'a seismic and exceedingly rare event' on a public one.[124] According to Werbach and Cornell, 'Because the only enforcement mechanism was the Ethereum network's computers executing ther terms of the The DAO software code, there was no way to distinguish between a legitimate string of transactions and one with malicious intent'.[125]

[119] Article 28(1) of the GDPR.

[120] V Gatteschi, F Lamberti and C Demartini, 'Technology of Smart Contracts' in LA DiMatteo, M Cannarsa and C Poncibò (eds), *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms* (Cambridge, Cambridge University Press, 2020) 54.

[121] K Werbach and N Cornell, 'Contracts Ex Machina' (2017) 67 *Duke Law Journal* 350.

[122] ibid 351.

[123] ENISA, 'Distributed Ledger Technology & Cybersecurity – Improving information security in the financial sector' (2017) 10, available at www.enisa.europa.eu/publications/blockchain-security/at_download/fullReport.

[124] Meyer (n 11).

[125] ibid 352.

Following a literature review, two scholars identified six security issues connected to smart contracts: 'transaction-dependency, timestamp dependency, mishandled exception, criminal activities, re-entrancy, and untrustworthy data feeds'.[126] These technical issues are too detailed to develop in this chapter, but suffice it to say, they need to be considered in design and development of smart contracts, which highlights the need for careful coding and dovetails with the GDPR requirement of 'data protection by design and by default', including 'data minimisation'.[127] According to ENISA,

> Smart contracts are essentially programs that run on the distributed ledger. They are prone to any faults associated with code. As with any software, the more complex a smart contract is, the more prone to software errors it will be.
>
> Generally, the function, and the security of smart contracts code depends on the author's capabilities.[128]

One technical means proposed to increase security in connection with use of the blockchain is to establish different private keys for signing and encrypting messages across the blockchain distributed ledger. This aspect of good 'key management' would ensure that even if a hacker were to obtain the private key for encrypting messages, and be able to read the data in the smart contract, they would not be able to modify them or otherwise interact with the smart contract.[129] Keys should be stored on secure media.[130] Reference has already been made to the use of cryptography, but the keys must be strong ones and a future threat is quantum computing, which should be taken into account for future-proofing the security measures.[131] ENISA recommends the following good practices as ways to mitigate privacy challenges related to limiting visibility of information to authorised entities and prevent unauthorised access to transactions:

(1) 'Encrypt the transactions, so only the involved counterparties can access the whole information';
(2) 'Use sharding to allow specific transactions to be validated by specific entities';
(3) 'Use pruning to remove data from the ledger at certain period of time, as requested by the regulation';
(4) 'In case an entity must be linked to a key, an authority may keep information of which key belongs to which entity'; and
(5) 'Encrypt ledger with more than one key.'[132]

[126] C Poncibò and LA DiMatteo, 'Smart Contracts: Contractual and Noncontractual Remedies' in LA DiMatteo, M Cannarsa and C Poncibò (eds), *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms* (Cambrdige, Cambridge University Press, 2020) 131.
[127] Article 25 of the GDPR. See section VII.B of this chapter.
[128] ENISA, 'Distributed Ledger Technology & Cybersecurity (2017) 18.
[129] ibid 14.
[130] CNIL (n 65) 10.
[131] ENISA (n 123) 14–15.
[132] ibid 21.

Now, this chapter turns to the purpose limitation and data minimisation concepts in the GDPR.

VII. Purpose Limitation and Data Minimisation

Two additional elements of the data protection principles merit brief attention here. These are the requirement of purpose limitation (section VII.A) and data minimisation (section VII.B).

A. Purpose Limitation

The purpose limitation data protection principle today may be seen to include both purpose specification for the data processing and use limitation. The GDPR provides that personal data shall be:

> [C]ollected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation').[133]

The first part of this principle – purpose specification – requires that there be clear communication to the data subject about the use of blockchain technology to process his or her personal data, including a 'specific and explicit' explanation that the data will be processed after the original transaction through the distributed ledger technology.[134] Finck comments that 'legitimate' purposes requirement means not only that there should be a legitimate grounds for data processing under Article 6 of the GDPR (Lawfulness of processing), but that the processing complies with broader applicable legal principles (eg non-discrimination).[135] Furthermore, in this light de Terwangne adds that the purposes 'may not entail a disproportionate interference with the rights, freedoms and interests at stake, in the name of the interests of the data controller'.[136]

The second part of the purpose limitation principle – use limitation (or compatible use) – calls for a case-by-case analysis, and Finck questions 'whether

[133] Article 5(1)(b) of the GDPR.

[134] M Finck, 'Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?' (European Parliamentary Research Service, 2019) 66, available at www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf.

[135] ibid 66.

[136] C de Terwangne, 'Article 5. Principles relating to processing of personal data', in C Kuner, LA Bygrave and C Docksey (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford, Oxford University Press, 2020) 315 (citation omitted).

there is a clear linkage of purpose of a single blockchain-based transaction and the continued storage and in the ledger',[137] which refers to the first of the criteria that will now be presented. Indeed, Article 6(4) of the GDPR sets out a list of criteria to be taken into account for a determination of the compatibility of the further processing, where it is not based on the data subject's consent:

(a) any link between the purposes for which the personal data have been collected and the purpose of the intended further processing;
(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;
(d) the possible consequences of the intended further processing for data subjects;
(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.[138]

B. Data Minimisation

Data minimisation is often referred to as part of the overriding data quality data protection principle. However, the GDPR separates it out. Personal data are to be 'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimisation")'.[139] Recital 39 not only repeats the text of Article 5(1)(c) of the GDPR, but adds that, 'Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means'.[140] Importantly, de Terwangne comments that 'one may not process an excessively large amount of personal data … But one may not process a single datum either if this would entail a disproportionate interference in the data subject's rights and interests'.[141] Thus, the limitation set out is not only quantitative, but also qualitative. Maxwell and Salmon remark that two features of the blockchain conflict with the data minimisation principle, as well as the storage limitation principle: data traveling through the blockchain are visible to every node and they cannot be deleted from the blockchain.[142] This principle is ripe for advisory guidance, according to Finck, which should include an analysis of the extent to which storing data off-chain may be a way to satisfy the data minimisation principle.[143]

[137] Finck, 'Blockchain and the General Data Protection Regulation' (2019) 67.
[138] Article 6(4) of the GDPR.
[139] Article 5(1)(c) of the GDPR.
[140] Recital 39 of the GDPR.
[141] de Terwangne, 'Article 5' (2020) 317.
[142] Maxwell and Salmon (n 25) 14.
[143] Finck (n 134) 68.

VIII. Cross-Border Data Transfers

The CNIL remarks that 'transfers outside of the European Union (EU) can be particularly problematic, especially in the case of public blockchains'.[144] In that context, participants and miners may span the globe, meaning that personal data could be located most anywhere, and potentially (more likely, probably) in jurisidictons outside the EU that do not benefit from an adequacy decision. Bacon, Michels, Millard and Singh echo this view, especially in the context of permissionless platforms:

> However, widely distributed, permissionless platforms are by design unconstrained by international border: typically anybody, anywhere, can download the entire transaction archive and start processing new transactions as a node or miner. As a result, use of these platforms is likely to entail data transfers to third countries. Since any party in any third country can download the archive, adequacy decisions and appropriate safeguards (including binding corporate rules) are unlikely to provide sufficient coverage.[145]

The CNIL reminds us that transactions on the blockchain involve 'a request to validate the transaction (and therefore potentially personal data) being sent to all miners of the chain' and updates through the addition of new blocks for all participants.[146] The CNIL recommends the use of permissioned blockchains in this regard:

> While appropriate safeguards for a transfer outside the EU may be used in a permissioned blockchain, such as standard contractual clauses, binding corporate rules, codes of conduct or even certification mechanisms, the CNIL observes that these safeguards are harder to implement in a public blockchain, given that the data controller has no real control over the location of miners.[147]

Finck likewise views the difficulties with cross-border transfers on a permissionless (public) blockchain. While on a private permissioned blockchain, it may be possible to obtain data subject consent to a cross-border transfer after providing information about the risks, based on controlled access and applicable terms and conditions, 'it is not obvious how such consent could be acquired in respect of a permissionless chain'.[148]

IX. Conclusion

Contrary to what some commentators may say, smart contracts and data protection legislation are not completely incompatible. However, a good undertstanding of the latter is necessary in order for smart contracts not to violate the legislation.

[144] CNIL (n 65) 5.
[145] Bacon, Michels, Millard and Singh (n 24) 47.
[146] CNIL (n 65) 5.
[147] ibid 5.
[148] Finck (n 134) 28.

This chapter has intended to provide information on some of the challenges of the GDPR through a general presentation of the legislation, followed by a discussion of personal data in the context of smart contracts, and then an analysis of some of the most relevant data protection principles and data subject rights.

Public blockchains provided several issues insofar as EU data protection law is concerned, especially in a B2C context. One solution may be to use only permissioned blockchains for B2C contracts, establishing the identity of the controller through contract. Indeed, the EU Blockchain Observatory is of the opinion that, 'a private permissioned blockchain network operated by a consortium of companies or by a government agency will be better position to apply the letter of the GDPR than a public blockchain network without permission'.[149] Avoidance of the use of personal data on the blockchain is another strategy, when possible, for example in the context of B2B smart contracts between legal persons. The chances of avoiding the use of personal data increase when business to consumer (B2C) transactions are excluded from the use of smart contracts. Next, proper anonymisation results in data no longer being considered 'personal' and thereby is a way to avoid the application of the GDPR, at least downstream, which is to say after the anonymisation.

Accountability is a concern, especially given the increased level of administrative sanctions possible under the GDPR and strengthened supervisory authority powers. In this light, finding the relevant party with responsibility is difficult. Generally, this will be the controller, who bears the brunt of most data protection obligations, although data processors also have potential liability. Defining the roles of the different actors in smart contracts using the blockchain requires careful analysis and the type of blockchain involved – whether this be a public permissionless one or a private permissioned blockchain – will be crucial in this regard.

This chapter has highlighted the main data subject rights that create difficulties in connection with smart contracts using the blockchain. These are essentially the right to rectification and the right to erasure ('right to be forgotten'), given the immutability of the blockchain. In addition, the right not to be subject to a decision based solely on automated processing was worth investigating. Elements of data protection principles – security ('integrity and confidentiality'), purpose limitation, data minimisation – are worthy of study, and have been the subject of sections of this chapter, as have issues related to the GDPR's cross-border personal data transfer requirements.

An industry association representative set out his formula for 'a GDPR-compliant Blockchain solution': 'Keep it private', 'Don't get personal' and 'Set the rules up front'.[150] In other words, stick with a private network, do not handle any personal information, and establish a clear 'common contractual governance framework'.[151] While making use of smart contracts using Blockchain technology GDPR-compliant is not an easy task, those rules provide a good starting point.

[149] Lyons, Courselas and Timsit (n 59) 16.
[150] Bailey, 'Blockchain And EU Privacy Laws' (2019).
[151] ibid.