Smart contracts as a form of solely automated processing under the GDPR

Michèle Finck*

Key Points

- Whereas Article 22 of the General Data Protection Regulation ('GDPR') prohibits solely automated data processing, the precise scope of this qualified prohibition as well as related requirements remain untested and unclear. Examining Article 22 GDPR from the perspective of smart contracts sheds light on the resulting uncertainties and inconsistencies.
- Smart contracts indeed appear to qualify as a form of solely automated data processing under Article 22(1) GDPR. This implies that they can only be used where they meet the requirements of Article 22(2) and implement the safeguards of Article 22(3) GDPR.
- Under Article 22(2) GDPR, solely automated data processing can only be used where it (i) is necessary for a contract between the data subject and controller, (ii) authorized by EU or Member State law, or (iii) based on the data subject's explicit consent. At first sight, these requirements can be met in the smart contract context just as in others. Yet, the research unveils that even where a smart contract is related to a legal contract, that contract may not be between the data subject and controller. Furthermore, consent may have limited value in this context as under EU data protection law, the data subject must be able to revoke consent, which is difficult where the data processing cannot be halted at the request of the data subject.
- Where the requirements of Article 22(2) GDPR are met, Article 22(3) requires that data controllers implement safeguarding measures including a right to human intervention by the controller. There are ongoing uncertainties and controversies regarding the scope of this obligation that also permeate the smart contract context. Yet, solutions are already being developed to create forms of smart contracts that may be responsive to these legal obligations, confirming the GDPR's innovation-shaping function.

In accordance with Article 22(1) of the General Data Protection Regulation ('GDPR') a data subject has the right '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'.[1] At a time where automated personal data processing is on the rise across all sectors of the economy, there remains significant uncertainty regarding the exact scope of this qualified prohibition and its implications for the data-driven economy.

The hesitation to subject individuals to machine-made decisions dates back to the early stages of the data economy. The drafters of the 1995 Data Protection Directive[2] (DPD) were already concerned that sophisticated software might be perceived as having 'an apparently objective and incontrovertible character' so that humans would no longer critically assess them.[3] To some, the absence of human intervention in decision-making indeed amounts to a violation of human dignity.[4] To address these concerns the 1995 Directive

* Michèle Finck, Senior Research Fellow, Max Planck Institute for Innovation and Competition, Munich, Germany. E-mail: michele.finck@ip.mpg.de

I am indebted to Mireille Hildebrandt and the participants in the Privacy and Identity Lab's November 2018 meeting for helpful comments and guidance.

1 Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016] OJ L119/1 (hereafter 'GDPR').

2 Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31 (hereafter 'DPD').

3 Amended Proposal for a Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data COM (92) 422 final at 26.

4 Meg Leta Jones, 'Right to a Human in the Loop: Political Constructions of Computer Automation & Personhood from Data Banks to Algorithms' (2017) 47 Social Studies of Science 216, 217.

enshrined a prohibition of automated processing resulting in profiling.[5] This was inspired by earlier references to such practices in national legislation such as Article 3 of the French Data Protection Act 1978.[6]

In contrast, the GDPR embraces a broader take and catches all forms of solely automated processing, irrespective of whether they include profiling or not.

In spite of its pivotal significance for the data economy, the precise contours of this provision remain largely undefined as it hasn't been tested in practice.[7] As the prohibition of solely automated data processing has been extended in law, in practice automated (although not necessarily solely automated) forms of data analysis are increasingly common. Many novel business models or practices are based on this method, which leverages increases in data volumes, computer processing power and sophisticated algorithms. Machine learning has been said to be 'eating the world' as it enables new analysis and activities that are progressively able to outperform human decision-making (at least from the perspective of cost and scale).[8]

Smart contracts, which are the focus of the present article, are one form of automated data processing that promise to generate efficiency gains while powering new markets and ventures. Smart contracts can be defined as self-executing code that automatically processes its inputs when it is triggered. While these mechanisms are most often discussed in the context of blockchain technology, the idea of automated execution is now also being experimented with in relation to other technical infrastructures and has arguably already been used in many contexts for a long period of time.[9] In blockchain networks automated execution is smart contracts' core value proposition. A smart contract is a small computer program that executes on each node (computer) of a blockchain network and this independently of the control of a single actor. If this form of automated execution qualifies as 'solely automated processing' for the purposes of Article 22(1) GDPR, the European data protection framework will be a decisive factor determining the extent to which smart contracts can be used in the EU. To date, so-called smart contracts have mostly attracted lawyers' attention from the perspective of contract law as the arguably ill-chosen terminology has led to confusion. Whereas a smart contract will only in some circumstances be connected to a legal contract, they always consist of automated data processing, raising the question of GDPR compliance.

In this article, I attempt to shed some light on whether smart contracts qualify as a form of solely automated data processing under the GDPR. I take smart contracts as my looking glass to better understand the inner workings of Article 22 as well as to evaluate the future of smart contracts in the European legal space. My analysis commences with an introduction to the relevant software. Thereafter, I examine Article 22 GDPR and test its application to smart contracts. My evaluation concludes with a survey of potential design choices that could bring smart contracts' solely automated processing and the GDPR's qualified prohibition thereof in alignment.

Smart contracts

Smart contracts are one of the buzzwords associated with blockchain technology. They have been defined as 'automated software agents hosted on blockchains that are capable of autonomously executing transactions on the triggering of certain conditions'.[10] In essence, a smart contract is self-executing computer code that automatically processes its inputs when triggered. Beyond, there is no universally accepted definition of these technical artefacts. While to some, they are just software code with the aforementioned characteristics, others insist on their contractual nature and legal implications. Furthermore, while smart contracts are conventionally discussed in relation to blockchains only, some are now starting to see smart contracts outside the confines of this domain.

The terminology dates back to 1994 when Nick Szabo described a smart contract as 'a set of promises, specified in digital form, including protocols within which the parties perform on these promises'.[11] Szabo envisaged software resembling contractual clauses.

5 Art 15 DPD.

6 Art 3 de la Loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ('Toute personne a le droit de connaître et de contester les informations et les raisonnements utilisés dans les traitements automatisés dont les résultats lui sont opposés').

7 Indeed, whereas art 15 of the Data Protection Directive enshrined an analogous right, this has never been subject to interpretation by the ECJ. See, however, the decision of the German Bundesgerichtshof BGH, *Schufa* case (8VU ZR 156/13) of 28 January 2014, holding that automated aspects of evidence only pertained to preparation of evidence whereas the decision to grant credit or not was made by a person.

8 Tom Simonite, 'Nvidia CEO: Software is Eating the World, but AI is Going to Eat Software' *MIT Technology Review* (12 March 2017).

9 On this, see further below.

10 Jake Goldenfein and Andrea Leiter, 'Legal Engineering on the Blockchain: "Smart Contracts" as Legal Conduct' (2018) Law and Critique (forthcoming), 2 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3176363> accessed 12 February 2019.

11 Nick Szabo, 'Smart Contracts: Building Blocks for Digital Markets' (1996) <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html> accessed 13 August 2018.

These artefacts would connect parties in a fashion that would make it difficult for one party to unilaterally terminate an agreement.[12] Others were similarly fascinated by the idea of creating contracts that could be read and utilized by humans and machines alike.[13] These visionaries however fell short of successfully implementing their visions. The idea experienced a revival around two decades later when Vitalik Buterin co-created the Ethereum blockchain. To Buterin, smart contracts are 'cryptographic "boxes" that contain value and only unlock it if certain conditions are met'.[14] From a technical perspective, smart contracts are thus simply 'computer programs that can be consistently executed by a network of mutually distrusting nodes, without the arbitration of a trusted authority'.[15] Indeed, Buterin recently announced: 'I quite regret adopting the term "smart contracts". I should have called them something more boring and technical, perhaps something like "persistent scripts"'.[16] In the meantime, however, the terminology has confused observers, lawyers and policy-makers alike, as much debate has focused on whether smart contracts are also legal contracts, possibly even requiring an adaptation of contract law.[17]

Because of their distributed execution, smart contracts are resilient to tampering, which makes them appealing in many scenarios including those that 'require transfers of money to respect certain agreed rules (like in financial services and in games)'.[18] Given that such smart contracts were designed for blockchain-based transfers of value, they are often examined in connection with legal contracts. Indeed to some, smart contract is 'a computer program that both expresses the contents of a contractual agreement and operates the implementation of that content, on the basis of triggers provided by the users or extracted from the environment'.[19]

Because smart contracts can indeed be used as a means of contractual execution, some consider that smart contracts are necessarily also legal contracts. A smart contract is however not necessarily smart nor a contract. Smart contracts are not 'smart' as they are unable to understand natural language (such as contractual terms) or to independently verify whether an execution-relevant event materialized. For this, oracles are needed. An oracle can be one or multiple persons, groups or programs that feed the software relevant information, such as whether a natural disaster has occurred (to release an insurance premium) or whether online goods have been delivered (to release payment).

Smart contracts also often cannot be qualified as contracts in the legal sense. Instead, they are usually a computer-programmable if-then relation unable to account for wider contextual factors. A smart contract is essentially a sequence of instructions that a blockchain miner runs in exchange for compensation.[20] As such, they are better defined as 'an autonomously executing piece of code whose inputs and outputs can include money'.[21]

The fact that smart contracts are neither smart nor contracts doesn't, however, imply that they are an insignificant tool. Rather, the opposite is the case. At least on blockchains where the appropriate governance set-up is given, smart contract code executes automatically and cannot be halted unless this option is specifically built into the code.[22] Even if one or a number or nodes fail, the software still executes on all remaining nodes, highlighting how blockchain achieves resilience through replication. Such automated execution enables transactions in situations devoid of human or institutional trust, lowers transaction costs and reduces counterparty risk and interpretative uncertainty.[23] Through smart

12 Ibid.

13 See Ian Grigg's Ricardian Contract. See <http://iang.org/papers/ricardian_contract.html> accessed 13 August 2018.

14 Vitalik Buterin, 'Ethereum White Paper. A Next Generation Smart Contract & Decentralized Application Platform' (28 March 2015) 13 <http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf> accessed 13 August 2018.

15 Massimo Bartoletti and Livio Pompianu, 'An Empirical Analysis of Smart Contracts: Platforms, Applications, and Design Patterns' in Michael Brenner and others (eds), *Financial Cryptography and Data Security* (Springer 2017) 494.

16 Vitalik Buterin [VitalikButerin] (13 October 2018) 'To be clear, at this point I quite regret adopting the term "smart contracts". I should have called them something more boring and technical, perhaps something like "persistent scripts"' [Tweet] <https://twitter.com/VitalikButerin/status/1051160932699770882?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1051160932699770882&ref_url=https%3A%2F%2Fwww.cryptoglobe.com%2Flatest%2F2018%2F10%2Fvitalik-buterin-regrets-promoting-term-smart-contracts%2Fwww.cryptoglobe.com%2Flatest%2F2018%2F10%2Fvitalik-buterin-regrets-promoting-term-smart-contracts%2F> accessed 12 February 2019.

17 See, by way of example, the current smart contract project of the UK Law Commission: <https://www.lawcom.gov.uk/project/smart-contracts/> accessed 24 April 2019.

18 Ibid.

19 Florian Idelberger and others, 'Evaluation of Logic-Based Smart Contracts for Blockchain Systems' in Jose Julia Alferes and others (eds), *Rule Technologies. Research, Tools, and Applications* (Springer 2016) 167.

20 This would however only be the case in respect of a blockchain that relies on a proof-of-work consensus algorithm.

21 Ari Juels, Ahmed Kosba and Elaine Shi, 'The Ring of Gyges: Using Smart Contracts for Crime' 2 <http://www.arijuels.com/wp-content/uploads/2013/09/Gyges.pdf> accessed 13 August 2018 (hereafter .

22 I return to such options further below. On blockchain governance, see further Michèle Finck, *Blockchain Regulation and Governance in Europe* (CUP 2018).

23 For an overview of smart contracts' advantages, see Mark Giancaspro, 'Is a "smart contract" Really a Smart Idea? Insights from a Legal Perspective' (2017) 33 Computer Law & Security Review 825; Richard Holden and Anup Malani, 'Can Blockchain Solve the Holdup Problem in Contracts?' (2017) 21–24 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3093879> accessed 13 August 2018.

contracts parties can moreover replicate elements of an existing contractual relationship through code.

Automated execution is accordingly smart contracts' main value proposition. Thomas Hobbes already emphasized that 'covenants, without the sword, are but words and of no strength to secure a man at all'.[24] Once an agreement has been translated into code, the intervention of a party or intermediary (other than the oracle) triggering contractual execution is replaced by the software's automated execution. Where smart contracts are used to automate the execution of contractual obligations, performance is hard-wired into the code. For example, the software can be used for the automatic transfer of collateral in the event of default or to disburse employee compensation if performance goals are achieved.[25] Other uses for smart contracts include InsurTech for event-driven insurance.[26] Smart contracts can be relied on to provide automatic compensation to policyholders where flights are delayed. In this scenario, the smart contract is connected to global air traffic databases (the oracle) and where these reveal a delay exceeding a pre-determined threshold, compensation is provided directly to the consumer.[27] Smart contracts may accordingly lead to more efficient consumer rights enforcement.[28] This potential has not gone unnoticed as the German government has set out to evaluate smart contracts in relation to consumer contracts.[29] Smart contracts thus offer the hope of a more efficient enforcement of law through technology, also illustrated by experiments using smart contracts as a means of ensuring tax compliance.[30]

Automated execution of course not only provides benefits but also disadvantages. Where software executes automatically, unwanted transactions can no longer be rolled back. This can be problematic, such as when a party lacks legal capacity or decides to default on its obligations. Modifications, such as those mandated by judicial decisions cannot be accommodated. Automated execution can also be useful for unlawful purposes such as the coordination of anti-competitive behavior including price-fixing and to 'effectively guarantee payment for committed crimes' and conversely to fuel criminal ecosystems.[31] Removing the ambiguity inherent in natural language by relying on rigid code also has disadvantages as flexibility indeed fulfils an important role in contractual settings (think of terms such as 'good faith' or 'best efforts' which cannot be expressed through computer language).

To date, smart contracts have been discussed mainly in relation to blockchain technology. As second-layer applications, smart contracts benefit from the tamper-proof nature of the underlying blockchain infrastructure that anchors their automated execution.[32] As many blockchain nodes run smart contract code, it 'is not controlled by—and cannot be halted by—any single party'.[33] Current excitement around the mechanism has however also triggered a parallel debate that considers that smart contracts could also be deployed on other technical infrastructures. Considering that smart contracts are little more than a deterministic if-then relation, it is plain that they have been a reality long before blockchain technology came along. From this perspective, '[a]n automated recurring payment that someone sets up with a bank is an example of a smart contract'.[34] Under this wider definition, smart contracts can be useful in variegated contexts. To illustrate, Digital Rights Management could be seen as an instance of a smart contract, as well as a bank's IT infrastructure. The technical details and governance of these systems and blockchains are however noticeably distinct as the latter are (at least in theory) set up in a manner to render unilateral human intervention in the system impossible, thus guaranteeing the occurrence of automated execution. In other systems, this is not necessarily a given.

Only time will tell how the terminology and usage of smart contracts will evolve. Just like electronic contracts have for a long time, smart contracts, whether used in a contractual setting or not, raise manifold legal

24 Thomas Hobbes, *Leviathan* (The Floating Press 2009) pt II Ch XVII 240.

25 David Yermack, 'Corporate Governance and Blockchains' (2017) 21 Review of Finance 7, 26.

26 Stan Higgins, 'AXA Is Using Ethereum's Blockchain for a New Flight Insurance Product' (*coindesk*, 13 September 2017) <https://www.coindesk.com/axa-using-ethereums-blockchain-new-flight-insurance-product/> accessed 13 August 2018.

27 'AXA goes blockchain with fizzy' (13 September 2017) <https://www.axa.com/en/newsroom/news/axa-goes-blockchain-with-fizzy> accessed 13 August 2018.

28 Martin Fries, 'Law and Autonomous Systems Series: Smart consumer contracts - The end of civil procedure?' (*Oxford Business Law Blog*, 29 March 2018) <https://www.law.ox.ac.uk/business-law-blog/blog/2018/03/smart-consumer-contracts-end-civil-procedure> accessed 13 August 2018.

29 'Koalitionsvertrag zwischen CDU, CSU und SPD' (12 March 2018) 124 <https://www.cdu.de/system/tdf/media/dokumente/koalitionsvertrag_2018.pdf?file=1> accessed 13 August 2018.

30 'Code as Law: Using Ethereum Smart Contracts to Ensure Compliance with Federal Tax Law' (*ConsenSys Media*, 29 May 2018) <https://media.consensys.net/code-as-law-using-ethereum-smart-contracts-to-ensure-compliance-with-federal-tax-law-3fc67cb7b956> accessed 13 August 2018.

31 Juels, Kosba and Shi (n 21) 1.

32 This is of course only the case to the extent that the blockchains' technical setup and governance arrangements guarantees this.

33 Primavera De Filippi and Aaron Wright, *Blockchain and the Law* (Harvard University Press 2018) 29.

34 Hanna Halaburda, 'Blockchain Revolution without the Blockchain' (2018) <https://www.bankofcanada.ca/wp-content/uploads/2018/03/san2018-5.pdf> accessed 13 August 2018.

questions.[35] What matters for our purposes is that in essence, smart contracts are mechanisms designed to achieve the automated execution of software code. This makes them a method of automated data processing. The GDPR, however, enshrines a qualified prohibition of solely automated data processing.

The GDPR's qualified prohibition of solely automated processing

Article 22(1) GDPR announces that data subjects have the right 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'.[36] To assess whether smart contracts are caught by this provision it must be determined whether (i) a smart contract counts as a decision based solely on automated processing, and (ii) whether that decision (a) produces legal effects for the data subject or (b) otherwise significantly affects him or her.

Decisions based on solely automated data processing

The GDPR doesn't define (solely) automated data processing.[37] For some time, there was uncertainty whether automated processing was merely a component of profiling or a separate thing altogether. Some indeed suggested that automated processing should not be seen as a freestanding practice triggering the application of the GDPR in the absence of profiling.[38] The contrary interpretation, it was suggested, would make the provision overly broad and go counter the focus on the harms associated with profiling in the preparatory works of the GDPR.[39]

In recent guidance, the A29WP opted for a textual interpretation of the provision, asserting that automated processing of data does not need to involve profiling to fall within the scope of Article 22.[40] Rather, it was argued that automated decision-making 'has a different scope and may partially overlap with or result from profiling'.[41] The guidance document also provides a definition of solely automated decision-making as 'the ability to make decisions by technological means without human involvement'.[42] A decision is hence 'based solely' on automated processing where there is 'no human involvement' in the decision-making process.[43] According to Goldenfein and Leiter, smart contracts' automated transaction can be thought of as 'a means of exchanging value in which some dimension of the actual exchange is processed by a machine, without human intervention'.[44]

The GDPR however only targets 'decisions' made through solely automated data processing. This raises the question whether a smart contract can be qualified as a decision. This is an example of the GDPR using terminology that may have certain common-sense understandings (as it also does in respect of other terms such as the 'logic' discussed below) without specifying what precise interpretation ought to be given to the term at issue. This interpretative challenge is augmented by the fact that whereas Article 22 only refers to 'decisions' reached by solely automated data processing, Recital 71 provides that data subjects have the right not to be subject to a 'decision, which may include a measure' based on solely automated data processing. The mentioning of measure in the preamble but omission thereof in the text of the GDPR likely simply echoes a lack of interinstitutional agreement over which terminology to use as the Commission's 2012 draft of the GDPR indeed only used the word 'measure' instead of 'decision' in Article 22[45], which was only subsequently introduced by the Council.[46] How these terms ought eventually to be interpreted will ultimately be clarified by the European Court of Justice.

35 See, by way of example, United Nations Convention on the Use of Electronic Communications in International Contracts.

36 My own emphasis.

37 Profiling is defined by art 4(4) GDPR as 'any form of automated processing consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements'.

38 Isak Mendoza and Lee Bygrave, 'The Right not to be Subject to Automated Decisions based on Profiling' in Tatiani-Eleni Synodinou and others (eds), *EU Internet Law: Regulation and Enforcement* (Springer 2017) 1.

39 Ibid 14.

40 A29WP, Guidelines on Automated Individual Decision-Making and Profiling.

41 Ibid 8.

42 Ibid.

43 Ibid 20.

44 Jake Goldenfein and Andrea Leiter, 'Legal Engineering on the Blockchain: "Smart Contracts" as Legal Conduct' (2018) Law and Critique (forthcoming), 4 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3176363> accessed 12 February 2019.

45 European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)' COM (2012) 11 final.

46 Bayerisches Landesamt für Datenschutzaufsicht, 'Synopse der DSGVO' <https://www.datenschutz-grundverordnung.eu/wp-content/uploads/2015/12/BayLDA_Synopse_DS-GVO_KOMM-EU-Parlament-Rat_160623TK.pdf > accessed 12 February 2019.

Some have suggested that whereas a 'decision' is an act or omission with legal consequences, a 'measure' is an act or omission with mere factual significance.[47] Whether this is indeed what the drafters had in mind can be questioned as Article 22 itself stipulates that decisions can have legal effects or otherwise significantly affect an individual. In any event, the fact that Recital 71 considers that a 'decision' can also be a 'measure' indicates that the term ought to be read widely.[48] The Court of Justice of the European Union ('CJEU') tendency to adopt a broad definition of different GDPR concepts (such as personal data or controllership) in order to guarantee the effective and complete protection of data subjects invites the same conclusion.[49]

At least where a smart contract leads to an outcome that would be reached through a human decision-making process in the analogue world should be considered as a 'decision'. This would be the case where a smart contract is used in InsurTech to decide on the release of an insurance premium. However, it is worth wondering if the use of a smart contract to operate a token sale or levy VAT similarly constitutes a 'decision'. It would appear that the discretionary elements that qualifies human decision-making is missing in contexts where something is mandated by law, even though individuals of course always have the option of non-compliance under the threat of related consequences. Nonetheless, similar uses of smart contracts may qualify as measures and still be brought within the ambit of EU data protection law.

The A29WP has provided examples of practices caught by Article 22(1). It mentions the imposition of speeding fines issued purely on the basis of speed camera evidence as an instance of solely automated decision-making without human involvement.[50] This is, like smart contracts themselves, a simple if-then relation that is initially modelled by humans and subsequently executed by a machine. This mechanism could even be qualified as a smart contract if one adopts a broad definition of the concept—just as biometric passport controls or cash machines. If such tools are confirmed to qualify as decisions for GDPR purposes then it is safe to assume that many smart contract use cases will be, too.

Beyond the terminological difficulty of knowing whether a smart contract qualifies as a decision or measure, one may also wonder what the correct timing of assessment is. One may consider that the 'decision' simply relates to the execution of the smart contract code upon occurrence of a pre-determined event such as a decision whether a given fact justifies payment or reimbursement of a given sum. In line with the very rationale of smart contracts, there is no human involvement at the stage of 'the decision', meaning that Article 22(1) applies to such software.

Alternatively, one could argue that the 'decision' encompasses a broader timescale and is inclusive of the initial decisions that resulted in the smart contract. Indeed, in many circumstances, humans will be agreeing on the purpose and set-up of the smart contract. Sometimes, a human will act as the oracle feeding the smart contract input data needed to execute. Furthermore, humans are also needed to translate human intention into computer code. Where a smart contract is connected to a legal contract (such as when a smart contract is used to automate elements of contractual compliance), the 'decision' could be understood to encompass initial contractual negotiations. Whereas this alternative interpretation appeals to those hoping to evade the ambit of Article 22(1), it is less likely to be successful if one considers that Article 22(2) enshrines an explicit exemption from the Article 22(1) prohibition where a smart contract is used to perform a contract.[51] If human involvement in the elaboration of the contract were to be taken into account for the purposes of the first paragraph, there would be no need for an explicit exemption to this effect in the second paragraph. Considering the text of Article 22 GDPR as a whole accordingly invites the conclusion that the 'decision' for the purposes of Article 22(1) is likely to be the eventual execution of the code only, which indeed occurs without direct human involvement.[52]

We may accordingly conclude that smart contracts are at least in some circumstances caught by Article 22(1) GDPR. As a consequence, the Regulation's qualified prohibition of automated data processing applies, however only where automated processing produces

47 Winfried Veil, 'Automatisierte Entscheidungen im Einzelfall einschließlich Profiling' in Sibylle Gierschmann and others (eds), *Kommentar Datenschutz-Grundverordnung* (Bundesanzeiger 2018) Rn. 58.

48 Whereas art 22 GDPR solely refers to decisions, Recital 71 reads: 'The data subject should have the right not to be subject to a decision, *which may include a measure*, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention'.

49 See, by way of example, Case C-131/12 *Google Spain and Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] EU:C:2014:317, para 34.

50 A29WP (n 40) 8.

51 See further below.

52 Humans are of course always involved in the set-up of the relevant technical system.

legal or otherwise significant effects on the data subject. This is the second element of the Article 22(1) test that I now turn to.

The production of legal or otherwise significant effects

Under Article 22(1) GDPR, data subjects are only entitled not to be subjected to decisions based on automated processing when the latter produce legal effects concerning them or similarly significantly affect them. It is accordingly necessary to enquire whether smart contracts can produce (i) legal effects, or (ii) similarly significant effects. This is to be determined on a case-by-case basis and there will be scenarios, such as machine-to-machine payments concerning the Internet of Things where there will be no (significant) effects on humans at all.

However, oftentimes smart contracts will have consequences for individuals, such as when they determine whether an insurance premium is paid, consumer rights are enforced or payment for a good or service is released. The A29WP has defined 'legal effects' as a change in legal rights or obligations, legal status or rights under a contract.[53] If a smart contract is used to execute a contractual obligation a change in legal rights and obligations occurs. Indeed, where a payment is executed or a tokenized good or title is transferred, the rights of one party and the obligations of another inevitably change. Many smart contracts will thus have legal effects and as a consequence be caught by Article 22(1).

Even where no legal effects are triggered, a smart contract's execution may nonetheless significantly affect a data subject. Under Article 22(1), a 'similarly significant effect' can be positive or negative and occurs where the consequences of automated data processing are 'sufficiently great or important to be worthy of attention'.[54] This is said to include significant effects on the circumstances, behaviour, or choices of the individual or a prolonged or permanent effect on the individual.[55] In itself this test isn't very helpful to demystify Article 22(1)'s scope of application as effects 'worthy of attention' vary greatly from one context and individual to another. For instance, an automated decision to grant someone access to a specific building (based on a chip or similar instrument) may be trivial in some circumstances yet vital in others (such as where a candidate wants to attend a job interview). Whereas there is no clear guidance on whether the existence of 'otherwise significant effects' is to be determined from an objective or subjective perspective, it appears safe to presume that an objective analysis is warranted as subjective analysis is impractical and would burden any data protection by design efforts.[56] To determine whether otherwise significant effects occur, a case-by-case analysis is needed but it is safe to conclude that this will be case in at least some instances.

It is worth noting that while 'similarly significant effects' excludes any effects that are unimportant from an objective standpoint, no de minimis threshold appears to apply to legal effects. If no de minimis standard is embraced, there is a risk that Article 22(1) becomes boundless. Such a maximalist reading could result in a scenario where any simple if-then relation with legal effects would be caught by the prohibition of automated processing, even where they are a far cry (think of a vending machine sale) from the examples of an automated refusal of an online credit application or automated recruiting practices without any human intervention, which are listed in Recital 71.

A further aspect that must be addressed is that of the necessary preconditions for forms of solely automated data processing to be caught by the GDPR. Indeed, there is room for speculation whether any solely automated data processing (irrespective of whether input data is personal data or not) is caught by Article 22 or whether there needs to be input data that qualifies as personal data for this to be the case. This is not evident from the wording of Article 22(1) which speaks of a decision being applied to 'the data subject'. This raises the question of what data makes the individual a data subject. One could argue that there is a need for input data to qualify as personal data. An example would be the examples mentioned in Recital 71, namely those of e-recruiting practices or automated credit assessment where the input data is indeed personal data. One may however wonder whether there can be situations where input data is not personal data and the output decision is so that Article 22 GDPR nonetheless applies.

The above analysis revealed that smart contracts are likely to at least in some scenarios fall within the scope of the GDPR's qualified prohibition of automated processing. This prohibition is not, however, absolute. While prima facie prohibited, automated processing can be justified on the basis of Article 22(2) GDPR.

53 A29WP (n 40) 21.

54 Ibid.

55 Ibid.

56 Veil (n 47) 665 (making the argument in favour of objective assessment).

II. Exceptions to the Prohibition of Automated Processing

The second paragraph of Article 22 GDPR foresees three distinct scenarios in which automated data processing remains lawful. I examine all three in turn and apply the different options to smart contracts. Note that I only engage with scenarios that do not involve sensitive data, as in such circumstances stricter conditions for processing apply.[57] According to Article 22(2) the prohibition of automated processing does not apply if the decision:

(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

(c) is based on the data subject's explicit consent.

The provision thus makes available three exceptions to the prohibition of automated processing under Article 22(1) GDPR.[58] First, it formulates that automated execution is tolerated where it is necessary for the entering into or performance of a contract between the data subject and the controller. We've observed above that the most discussed potential for smart contracts resides in the automated execution of (elements of) legal contracts.[59] Where the smart contract is chosen to perform a contractual obligation, automated processing in the form of self-executing code can be relied upon.

This, however, presupposes that the existing legal contract is concluded between the data subject and the data controller. Initially, the legislative proposal of the Commission and the Parliament merely mentioned that automated execution must be part of the execution of a contract. It was the Council that suggested that this contract must occur between the controller and the data subject, which has been reflected in the final version of the Regulation.[60] In many scenarios this will not cause difficulty. For example, where a bank uses a smart contract to execute clients' automated recurring payments, the bank is a party to the contract, and at the same time the data controller in relation to the client's personal data.

Where public and permissionless blockchains that can be read and used by anyone are used to execute the smart contract, the requirement that the contract be concluded between the data subject and the data controller creates significant complication.[61] In such a scenario, personal data may be found in various locations. Most of the personal data relating to the client will be with the provider. However, smart contracts may also be considered to be personal data for the purposes of Article 22 GDPR where they generate a decision that is applied to the data subject where this results in data that directly or indirectly relates to an identified or identifiable natural person. Further, public keys, the pseudonymous identifiers on blockchains likely also qualify as personal data.[62]

Under the GDPR, a data controller is the entity that determines or co-determines the means and purposes (the 'why and how') of personal data processing.[63] It has become plain that a broad definition of this concept ought to be applied.[64] Recently, the Grand Chamber held in *Wirtschaftsakademie Schleswig Holstein* that administrators of a Facebook fan page are joint controllers (together with Facebook) regarding some of the data subjects' personal data.[65] The Court opined that the notion of a controller must be interpreted broadly to guarantee the effective and complete protection of data subjects.[66] As a consequence, the administrator of a fan page hosted on Facebook 'must be regarded as taking part, by its definition of parameters depending in particular on its target audience and the objectives of managing and promoting its activities, in the determination of the purposes and means of processing the personal data of the visitors to its fan page'.[67]

It thus appears that where a smart contract is used, the blockchain system that is relied on also constitutes a data controller. Yet, public and permissionless systems are not steered by a single legal entity that could easily be designated as the controller. Rather, these decentralized systems are shaped by the collaboration of a multitude of actors including nodes, miners, users and core

57 See further art 22(4) GDPR.

58 These might be further specified in the future in accordance with art 70(1)(f) GDPR.

59 Recital 71 GDPR also provides that automated decision-making should be allowed where 'necessary for the entering or performance of a contract'.

60 See further Marcus Helfrich, 'Artikel 22' in Gernot Sydow (ed), *Europäische Datenschutzgrundverordnung* (Nomos 2017) 570.

61 For instance, Axa uses the public and permissionless Ethereum network to manage smart contracts in relation to a flight insurance product. 'AXA goes blockchain with fizzy' (13 September 2017) <https://www.axa.com/en/newsroom/news/axa-goes-blockchain-with-fizzy> accessed 13 August 2018.

62 See further Michèle Finck, 'Blockchains and Data Protection in the European Union' (2018) 4 European Data Protection Law Review 17.

63 Art 4(7) GDPR.

64 Case C-131/12 *Google Spain* [2014] EU:C:2014:317.

65 Case C-210/16 *Wirtschaftsakademie Schleswig Holstein* [2018] EU:C:2018:388.

66 Ibid, paras 28 and 56. See also Case C-131/12 *Google Spain* [2014] EU:C:2014:317.

67 Ibid, para 39.

developers and there remains uncertainty as to who qualifies as the controller from the perspective of the GDPR.[68] The French Data Protection Authority recently suggested that smart contract developers can also be deemed data controllers in some circumstances.[69]

Whereas the precise identity of the data controller has to be determined in light of a given blockchain's specific governance set-up, it appears unavoidable to conclude that actors situated at the infrastructure layer (the blockchain) as well as those at the application layer (the smart contract) are likely joint-controllers under the GDPR. Further, there is an argument to be made that the person holding the private key to the smart contract could also be a joint controller.[70] Whether these complexities constitute a problem in relation to the invocability of Article 22(2)(a) is however another question. While guidance is as of yet missing on this point it appears reasonable to assume that the existence of a contractual relation with at least one of multiple controllers would be sufficient to invoke this exemption.

Beyond, it is worth pondering the meaning of 'necessary' as Article 22(2)(a) foresees that solely automated data processing may occur where it 'is necessary for entering into, or performance of, a contract between the data subject and a data controller'.[71] While the specific interpretation of this terminology remains somewhat unclear at this stage, it could be understood to mean that solely automated processing should only be used where no alternative decision-making processes are available.[72] Yet, whether such an extreme interpretation is mandated can be questioned on the basis of the examples of solely automated data processing found in the preamble, namely that of a credit application and automated recruiting practices.[73] These examples indicate that, the threshold of necessity applied should be low indeed as credit evaluations and recruitment procedures are very well possible in the absence of automation. On the other hand, the A29WP has considered that automation is not 'necessary' where 'other effective and less intrusive means to achieve the same goal exist'.[74] While this indicates that necessity ought to be interpreted narrowly, the example provided by the A29WP doesn't abide by the strict threshold it announces. Indeed, the A29WP notes in relation to pre-contractual processing that where an employer receives 'tens of thousands' of applications for a job opening, then this exceptionally high volume of applications may make automated decision-making necessary as a first step in the process. Whether this is really 'necessary' is a question to be asked though, as the same outcome could be reached through non-automated means, even though it would of course take more time. There accordingly remains uncertainty regarding the scope of necessity, and particularly whether parties can agree that something is necessary in the name of contractual freedom or whether objective standards should prevail.

Article 22(2)(b) GDPR furthermore authorizes Member States or the EU to create exemptions to the prohibition of automated processing provided that data subject rights and interests are safeguarded.[75] At this stage, no legislation has been passed at EU or Member State level to enable solely automated data processing in relation to smart contracts. At the same time, Member States wishing to attract related industries to their territory may rely on Article 22(2)(b) GDPR for these purposes. The particular attractiveness of this option resides in the fact that the requirements arising under Article 22(3) GDPR, examined below, do not apply.

Article 22(2)(c) GDPR allows automated data processing where it is based on the data subject's explicit consent. Where there is an analogue contractual relationship preceding the smart contract this can be implemented in a straightforward manner as explicit consent could be acquired on the same occasion as the contract is signed. It can be harder in other contexts such as current forms of token sales where there is often no parallel legal contract to the smart contract. However, at least in the abstract it should also be possible to gather consent in such circumstances.[76] Two points are worth highlighting in this respect. First, the language of 'explicit' consent, which is not defined in the GDPR.[77] It has been interpreted by the A29WP in its guidelines on consent as necessary in situations that involve serious data protection risks so that 'a high level of individual control over personal data is deemed appropriate'.[78] Regular consent required a 'statement or clear affirmative action' on behalf of the data subject. Where 'explicit' consent is needed in view of the high risk of personal data processing, the data subject 'must give an

68 See further Finck (n 62) 17.

69 CNIL, 'La Blockchain'. Premiers éléments d'analyse de la CNIL, Septembre 2018.

70 See further below.

71 My own emphasis.

72 Art 22(2)(a) GDPR creates thus a higher standard than what was previously required under Article 15(2)(a) of the Data Protection Directive.

73 Recital 71.

74 See A29WP (n 40) 23.

75 As Germany has done in respect of the insurance sector.

76 See art 7 and Recital 32 GDPR.

77 The GPDR refers to both 'consent' and 'explicit' consent. Key provisions on consent such as Recitals 32 and 43 as well as arts 4(11) and 7 GDPR don't however provide information as to what the differences between both categories are and only 'consent' is defined in art 4(11) GDPR.

78 Art 29 Working Party Guidelines on Consent WP259 (2018), 18.

express statement of consent' which could take the form of a written statement or the filling in of an electronic form or scanned documents using online signatures.[79] Data controllers are further encouraged to use two stage verification of consent.[80] The threshold of consent required is thus a high one. Secondly, Article 7 GDPR requires that the data subject has 'the right to withdraw his or her consent at any time'.[81] While this may not affect the lawfulness of processing based on consent that occurred prior to withdrawal, this requirement causes difficulty in the case of automated data processing as, unless this is explicitly foreseen, it may be difficult for a data subject to put an end to the data processing in revoking consent. In such scenarios and in the absence of another lawful basis that justifies data processing (such as further storage), personal data should be deleted by the controller, which brings us to the difficulty of amending or deleting data in blockchains. These complications indicate that data controllers wishing to rely on consent as a basis for lawful personal data processing will face significant hurdles.

Article 22(2) accordingly provides a number of options to lawfully operate smart contracts under EU law. Where this is the case, certain requirements must however be respected. Indeed, if reliance on automated processing occurs under Article 22(2)(a) or (c), safeguarding measures apply in the form of a right to human intervention (under Article 22(3) GDPR) and a right to be informed (under Articles 13 and 14 GDPR).[82] The A29WP has moreover recalled that where automated processing involves a high risk, a Data Protection Impact Assessment ('DPIA') may be desirable.[83]

3. The Right to Human Intervention

Article 22(3) mandates that where automated processing is authorized on the basis of the first or third part of Article 22(2), the data controller shall implement suitable measures to 'safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision'.[84]

EU data protection law thus only allows automated data processing where it is not, in fact, purely automated.[85] The provision is indeed based on a circular reasoning whereby Article 22(1) only applies where processing occurs through solely automated means without the option of human intervention, yet by virtue of Article 22(3) processing can never be solely automated anyways.[86] Article 22(3) enshrines an obligation that automated data processing can only occur under Article 22(2)(a) or (c) where there is an option of human intervention on behalf of the controller and the data subject's rights, freedoms and legitimate interests are adequately protected. Whereas the precise contours of the latter aspect are subject to debate, the possibility of human intervention is an unavoidable requirement. Data subjects are of course free to not rely on the option of human intervention, allowing for conditional solely automated data processing under the GDPR. Applying this to smart contracts, three questions emerge. First, what is human intervention; second at what stage must it be available; and third is the data controller in a position to provide it?

First, it is appropriate to enquire what shape human intervention must take to satisfy the conditions of the EU's data protection framework. The A29WP has underlined that human intervention must not just be nominal but rather take the form of a review carried out by someone who 'has the appropriate authority and capability to change the decision'.[87] The reviewer should 'undertake a thorough assessment of all the relevant data, including any additional information provided by the data subject'.[88] The A29WP's warning that human intervention should not just be nominal is important. Research has revealed that humans tend to trust decisions made by algorithms and assume their validity even where there is evidence that it is erroneous.[89] Further, even where a system is designed as a human support system rather than as a completely autonomous

79 Ibid.

80 Ibid 19.

81 Art 7(3) GDPR.

82 A29WP (n 40) 20.

83 Ibid.

84 Art 22(3) GDPR.

85 With the exception of cases caught by art 22(2)(b) GDPR.

86 In the words of the A29WP '[t]he term 'right' in the provision does not mean that Article 22(1) applies only when actively invoked by the data subject. Art 22 (1) establishes a general prohibition for decision-making based solely on automated processing'. See further art 29 Data Protection Working Party, Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679 WP251rev.01 (6 February 2018) 19 (hereafter 'A29WP, Guidelines on Automated Individual Decision-Making and Profiling').

87 A29WP, ibid 27.

88 Ibid.

89 Mary Cummings, 'Automation Bias in Intelligent Time Critical Decision Support Systems' (AIAA 1st Intelligent Systems Technical Conference, Chicago, 20–22 September 2004) <https://arc.aiaa.org/doi/10.2514/6.2004-6313> accessed 13 August 2018; Kathleen Mosier and others, 'Automation Bias: Decision Making and Performance in High-Tech Cockpits' (1997) International Journal of Aviation Psychology 47. It is worth noting that such assumptions may however be changing as a consequence of increased awareness regarding the shortcomings of such processes.

decision-maker, it may still be used as the latter where the human lacks time, chooses convenience or trusts the machine's judgment.[90] Clearly, the factual must trump the formal in determining whether human intervention occurs.

There is another noticeable aspect to this guidance, namely that it is sufficient that human intervention occurs after the decision has been taken—not necessarily in the course of the decision, as a means of halting it.[91] In the smart contract context, we could imagine processes that review the outcome of the smart contract once it has been executed. From a purely technical standpoint, this is relatively straightforward as reading a coded if-then relation is easy for the technically skilled. When it comes to the readability for purposes of human intervention, smart contracts are thus easier to align with the GDPR compared to other domains of automated decision-making such as deep learning models.[92]

In contrast to technical feasibility, the practical modalities of human intervention for the purposes of Article 22(3) may be harder for smart contracts to satisfy. Subjecting a smart contract to human intervention in a traditional corporate setting, such as in InsurTech or supply chain settings, can easily be implemented as the smart contract is but a technical utensil assisting processes steered by humans. In other contexts, such as those fashioned explicitly to be divorced from human governance, this is less readily implementable. Consider for instance the case of a smart contract governing a token purchase or, even more complicated, a Decentralized Autonomous Organization.[93] Here, entry points for human intervention are harder to identify as these systems may be designed with the aim to exclude human intervention.

Finally, attention must be paid to Article 22(3)'s requirement that the data controller orchestrate human intervention. As observed above, the identity of the data controller remains uncertain particularly in respect of public and permissionless blockchains and there is an argument to be made that there will be a number of joint controllers at infrastructure and application levels qualify as a controller. Whether an option of human intervention must be provided by all these parties, or only one of the various joint-controllers is an important question that merits clarification. Article 26 GDPR governs joint-controllership and requires that various controllers conclude an agreement that sets out their respective responsibilities.[94] Notwithstanding the details of that agreement, the data subject can however exercise her rights against any controller.[95] This would indicate that all controllers are liable to comply with the requirement of human intervention. However, it appears that the CJEU is considers that all data controllers don't necessarily have equal responsibility but that the responsibility of each controller 'must be assessed with regard to all the relevant circumstances of the particular case'.[96] Where solely automated processing occurs, the data subject is furthermore entitled to obtain information about this variant of data processing.

The right to be informed about solely Automated Processing

Where automated processing occurs, the data subject has a right to be informed about this fact. What exactly such information should encompass however remains subject to vivid debate. Article 12(1) GDPR requires that the controller provide data subjects with concise, transparent, intelligible and easily accessible information about the processing of their personal data. How this 'right to be informed' plays out in relation to automated data processing hinges on the relationship between Articles 13, 14 and 15 as well as Recital 71 GDPR. Article 13(2)(f) GDPR provides that a data subject is entitled to be informed about

> the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Article 14(2)(g) GDPR imposes the same requirement in circumstances where personal data was not obtained directly from the data subject.[97] The same wording is also reiterated by Article 15(1)(h) GDPR.[98] These provisions require that three distinct categories of

90 Linda Skitka and others, 'Accountability and Automation Bias' (2000) 52 International Journal of Human-Computer Studies 4, 701.

91 The A29WP speaks of a 'review' of the decision reached by automated means. See A29WP, Guidelines on Automated Individual Decision-Making and Profiling (n 86) 27.

92 This is unless smart contracts are combined with more complicated forms of automated data processing.

93 In essence, a DAO is a nexus of smart contracts. It has been defined as 'autonomous and algorithmic systems that rely on software algorithms to control access to assets and resources'. See further Primavera De Filippi and Aaron Wright, *Blockchain and the Law* (Harvard University Press 2018) 146.

94 Art 26(1) GDPR.

95 Art 26(3) GDPR.

96 Case C-210/16 *Unabhängiges Landeszenrum für Dateschutz Schleswig-Holstein v Wirtschafsakademie Schleswig-Holstein GmbH* [2018] EU:C:2017:796, para 43. See also *Jehovan Witnesses*, para 66.

97 Art 14(2)(g) GDPR.

98 Art 15(1)(h) GDPR reads as follows: 'the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject'.

information be provided to the data subject. Information about the (i) existence of automated decision, (ii) information about the involved logic and (iii) the significance and the envisaged consequences of the operation. Recital 71 appears to add a requirement to the right to information as it is dealt with in these provisions. It foresees that in instances of solely automated processing, a data subject shall benefit from 'suitable safeguards' including the right 'to obtain an explanation of the decision reached after such assessment and to challenge the decision'.[99] Whereas the term 'logic' can be difficult to interpret as it is not clear what meaning was intended by the drafters of the GDPR and this hasn't been clarified by the CJEU, Recital 71 may be understood as an indication that logic refers to an explanation of the precise ways in which how a decision is made. Such information is to be provided by the data controller, meaning that the same difficulties of identification examined above also arise in this context.

There has been much discussion as to the interpretation of the four different elements of information in the legislative text and its preamble. The requirement of 'explanation' in Recital 71 presumably goes further than what is enshrined in the legislative body. The status of a recital, however, is unlike that of a legislative provision. Recitals are not legally binding imperatives but rather interpretative aids.[100] They are designed to inform the interpretation of the legislative body and can change its meaning, with the limitation that they cannot be used for a contra legem interpretation of the latter. When the GDPR was negotiated, 'as a matter of political expediency, many issues too controversial for agreement in the main text have been kicked into the long grass of the recitals, throwing up problems of just how binding they are'.[101] These uncertainties have led to debates as to what exact information duties are mandatory under the GDPR. For instance, one may wonder whether the GDPR creates a duty to disclose algorithms that may enjoy trade secret protection to data subjects.

Over the past few years, a heated academic debate has unfolded regarding the contours of the GDPR's right to information/explanation. In a first (non-legal) conference paper, Goodman and Flaxman asserted that the GDPR creates a 'right to explanation', which, in their words, would entail 'human-intelligible explanations of algorithmic decision-making'.[102] As a reaction, Wachter et al wrote an article entitled 'Why a Right to Explanation of Automated Decision-Making does not exist in the General Data Protection Regulation' claiming that there is only a right to information that, in their opinion, only exists as an ex ante right for be informed about the existence of an algorithmic system rather than an ex post right to be briefed about how an automated decision was generated.[103] These authors maintained that the apparent disconnect between Recital 71 and Article 22 stems from the fact that while originally, a right to an explanation was considered for Article 22 this was dropped in the course of trilogue negotiations.[104] The omission from the final text was thus intentional, barring a wide interpretation thereof in line with Recital 71.

Their exposé was subsequently called into doubt by other scholars. Commandé and Malghieri put forward that Articles 13-15 and 22 should be interpreted systemically, revealing that they provide an opportunity for auditing algorithms.[105] Whereas trade secret protection may limit a data subject's right to open algorithmic black boxes, they maintained that the impact of trade secret protection should be reduced to favor data protection rights.[106] Selbst and Powles subsequently advocated a return to textual analysis and warned that the debate shouldn't focus on whether the concerned right should be termed a right to 'information' (as indicated by Articles 13-15) or a right to 'explanation' (the wording used in Recital 71 only) but that rather a functional interpretation allowing data subjects to exercise their rights should be preferred.[107] Edwards and Vaele moreover rightly stressed the limits of an alleged right to an explanation as a remedy where people feel they have been wronged by an algorithm.[108]

Ultimately, the ECJ will have the final word as to how these different concepts ought to be interpreted. In the

99 Recital 71 GDPR (my own emphasis).

100 Case C – 355/95 *TWD v Commission* [1997] EU:C:1997:241, para 21. See also Roberto Baratta, 'Complexity of EU Law in the Domestic Implementing Process' (2014) 2 The Theory and Practice of Legislation 293.

101 Lilian Edwards and Michael Vaele, 'Slave to the Algorithm? Why a "Right to an Explanation" is Probably not the Remedy You are Looking For' (2017) 16 Duke Law & Technology Law Review 18, 50.

102 Bryce Goodman and Seth Flaxman, 'European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation"' (28 June 2016) 5 <https://arxiv.org/abs/1606.08813> accessed 13 August 2018.

103 Sandra Wachter and others, 'Why a Right to Explanation of Automated Decision-Making does not exist in the General Data Protection Regulation' (2017) 7 International Data Privacy Law 76.

104 Ibid 81.

105 Gianclaudio Malgieri and Giovanni Comandé, 'Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation' (2017) 7 International Data Privacy Law 243.

106 Ibid.

107 Andrew Selbst and Julia Powles, 'Meaningful Information and the Right to Explanation' (2017) 7 International Data Privacy Law 233.

108 Lilian Edwards and Michael Vaele, 'Slave to the Algorithm? Why a "Right to an Explanation" is Probably not the Remedy You are Looking For' (2017) 16 Duke Law & Technology Law Review 18.

meantime, the A29WP has provided (non-legally binding) guidance on these matters. It considers that what is required of data controllers is that they (i) tell the data subject that they are engaging in solely automated processing, (ii) deliver meaningful information about the logic involved, (iii) and explain the processing's significance and envisaged consequences.[109] The information provided to these ends should include details about the categories of data used; why these data are seen as pertinent; how profiles are built; why the profile is relevant for the decision-making process and how it is used to reach a decision about the data subject.[110] The last three criteria appear to apply to profiling only.

Information in respect of the 'logic' that is used is understood as 'simple ways to tell the data subject about the rationale behind, or the criteria relied on in reaching the decision'.[111] Indeed, what is required is 'not necessarily a complex explanation of the algorithms used or disclosure of the full algorithm'.[112] Nonetheless, the information transmitted to the data subject should be sufficiently comprehensive to 'understand the reasons for the decision'.[113] Whether these explanations are a significant help in clarifying the current terminological confusion is a matter of debate. Indeed, the A29WP appears to be saying that explanation of algorithms or disclosure of the full algorithm isn't 'necessarily' required, implying that in some cases it might be. What such circumstances would be, however, is not elaborated. In any event, the controller ought to find 'simple ways to tell the data subject about the rationale behind, or the criteria relied on in reaching the decision'.[114] This could include the provision of counterfactual explanations, which could help individuals understand how the decisions or measures were reached without a need for opening the algorithmic black box and potentially violate trade secrets.[115]

Regarding the implementation of these requirements in a smart contract context two points should be distinguished. First, given that these obligations rest on the data controller the same complications as observed above apply. Secondly, the actual implementation of the obligation should be straightforward. Smart contracts in the form momentarily discussed don't involve large quantities of data and the logic involved in processing them is usually a simple deterministic if/then relation that can easily be explained, and likely doesn't enjoy trade secret protection.

It is worth pinpointing the connection between the right to information and the ability to legitimize automated processing through explicit consent under Article 22(2)(c). Indeed, one may wonder what level of information is required in order to for consent to be possible. Where the details of automated processing are not properly understood, it may be argued, consent cannot be objectively provided. This may result in a situation where more detailed information is required under Article 22(2)(c) as a consequence of the obligation to inform the data subject of some elements of data processing. This is an issue of broader magnitude as ongoing technical developments such as machine learning have raised concerns as to how humans can 'conduct a meaningful review of a process that may have involved third-party data and algorithms (which may contain trade secrets), pre-learned models, or inherently opaque machine learning techniques'.[116] There is thus a wider concern regarding how current and future automated decision-making processes can be rendered explainable and understandable, which is why effort is put into the development of explainable Artificial Intelligence ('XAI').[117] In some instances, data controllers that rely on smart contracts will also be subject to a duty to carry out a Data Protection Impact Assessment ('DPIA').

5. Data Protection Impact Assessments

In some circumstances, reliance on automated processing triggers an obligation to carry out a Data Protection Impact Assessment. DPIAs are evaluations of the impact of the planned processing operations on data subjects that ought to be carried out by data controllers where the the nature, scope, context and purposes of processing are of high risk to the rights and freedoms of natural parties, which can be the case in particular where new technologies are used.[118]

Under Article 35 GDPR DPIAs are recommended in particular where processing involves (i) a systemic and

109 A29WP, Guidelines on Automated Individual Decision-Making and Profiling (n 86) 25.

110 Ibid 31.

111 Ibid.

112 Ibid (my own emphasis).

113 Ibid.

114 Ibid 25.

115 For an overview, see Sandra Wachter and others, 'Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR' (2018) 31 Harvard Journal of Law & Technology 841.

116 Christopher Kuner and others, 'Machine Learning with Personal Data: is Data Protection Law Smart Enough to meet the Challenge?' (2017) 7 *International Data Privacy Law* 1, 2.

117 Tim Miller, 'Explanation in Artificial Intelligence: Insights from the Social Sciences' (22 June 2017) <https://arxiv.org/abs/1706.07269> accessed 13 August 2018.

118 Art 35(1) GDPR.

extensive evaluation of personal aspects of natural persons based on automated processing; (ii) sensitive data and data related to criminal convictions and offences or (iii) where the systematic monitoring of a publicly accessible area on large scale is involved.[119] Where a DPIA indicates that processing results in a high risk for data subjects and no measures to mitigate the risks can be taken, the controller is required to inform the supervisory authority.[120]

At first glance, nothing invites the conclusion that a DPIA must precede the execution of a smart contract. Indeed, while such assessments are needed where automated processing occurs (note that Article 35 refers to 'automated processing' not 'solely automated processing' as Article 22) this is only the case where processing involves a systemic and extensive evaluation of personal aspects of natural persons. Similarly, it cannot be said that as a general matter, the nature, scope, context and purposes of processing are of high risk to the rights and freedoms of natural parties.

It could, however, be argued that in some circumstances, smart contracts are a 'new technology' requiring a DPIA. Arguing that smart contracts are, as such, a new technology would be nonsensical. The if/then relation characteristic of smart contracts has long been relied on in contexts such as in vending machines, financial transactions or automated boarding pass and passport controls. However, where a smart contract is deployed on a blockchain, particularly if of a public and permissionless nature, there are compelling reasons to carry out a DPIA as this infrastructure itself constitutes a new technology that involves a high risk from a data protection perspective. While it builds, like any innovation, on previously existing components, a blockchain (especially where public and permissionless) is considerably distinct from other database structures in some ways. Further, due to some of the very characteristics of blockchains, such as their inherent transparency and lack of anonymity, reliance on these systems might be classified as presenting a high risk for data protection.[121] Ultimately, a DPIA is an exercise in risk management so that a case-by-case analysis ought to be carried out to determine the precise risks for the data subject as they result from the specific technical and governance setups. A DPIA can also be carried out as an important step in complying with the data protection by design imperative.

Data protection by design and data protection by default

Article 25 GDPR requires the integration of the two core data protection principles of data protection by design and data protection by default into any personal data processing system.

Article 25(1) GDPR requires that controllers implement appropriate technical and organizational measures to meet the GDPR's requirements, both at the time of processing as well as when determining the means of processing. In this context, the 'state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing' ought to be taken into account.[122] In particular, the GDPR creates a duty for the controller(s) to implement appropriate technical and organizational measures (meaning that the design requirements do not just apply to the actual technical processing but also to the business model as such) to make sure that only the data 'necessary for each specific purpose of the processing' are processed.[123]

The rationale behind these requirements is that system architecture may be a more efficient means of achieving compliance compared to the simple existence of normative postulates.[124] As such, it is 'an ambitiously conceived provision that seeks to reach into the heart of the machinery of our information age and reshape it to respect important values'.[125] The concept has origins in the softer requirement of the Data Protection Directive that appropriate technical and organizational measures ought to be taken in systems design to prevent unauthorized processing and maintain security.[126] It also is a close cousin of 'Privacy by Design' as it is discussed internationally.[127] Recital 78 clarifies that needed in particular are measures that minimize data processing, the

119 Art 35(3) GDPR.

120 Art 36(1) GDPR.

121 Under arts 35(3) and (4) GDPR supervisory authorities can publicize whitelists and blacklists of processing activities for which DPIAs are required, which however focus on given risk factors rather than specific technologies.

122 Art 25(1) GDPR.

123 Art 25(2) GDPR.

124 See further Lee Bygrave, 'Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements' (2017) 4 Oslo Law Review 105; Joel Reidenberg, 'Lex Informatica: The Formulation of Information Policy Rules through Technology' (1997) 76 Texas Law Review 553; Lawrence Lessig, *Code: and Other Laws of Cyberspace* (Basic Books 1999).

125 Bygrave, ibid 119.

126 Recital 46 of the Data Protection Directive.

127 See by way of example Ann Cavoukian, 'Privacy by Design: The 7 Foundational Principles' (August 2009) <https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf> accessed 13 August 2018.

pseudonymization of data, enabling a data subject to monitor data processing and security features created and improved by the controller.

These obligations have implications for smart contracts. Article 25 GDPR triggers an obligation for those offering such services to design this software as well as the IT infrastructure they rely on in a manner compatible with the GDPR overall, not just Article 22. Indeed, the requirements of data protection by design and data protection by default might make developers think twice when considering deploying their smart contract code on a blockchain.[128] This is so because blockchains are fashioned in a manner that makes compliance with core principles of the GDPR burdensome.[129] For example, it is difficult for such systems to meet the data minimization requirement (as they are a continuously expanding collection of data) or to implement data subject rights such as they rights to modification and erasure (as they are designed to prevent human intervention).[130]

In light of these uncertainties, reliance on Article 25(3) GDPR, which foresees the possibility of approved certification schemes as an element to demonstrate compliance with the data protection by design and data protection by default requirements becomes attractive, no such schemes have been initiated to date. Certification mechanisms are appealing since the exact scope of Article 25 GDPR remains somewhat unclear as the CJEU has not yet ruled on the matter and the provision itself is formulated in a broad manner. Compliance with these provisions is nonetheless pivotal as it is a factor taken into account when determining the imposition of fines for breaches of the GDPR.[131]

The above analysis has divulged that the GDPR's prohibition of solely automated processing applies to smart contracts. Whereas reliance on automated smart contracts can be justified where it is necessary in a contractual setting, is authorized by law, or where the data subject consents to the processing, systems and processes must be designed in a data protection friendly manner. This includes the availability of human intervention, the provision of information regarding the modalities of processing and, in some circumstances, a DPIA. As in all circumstances, smart contract operators must also be organized in a manner that accounts for the data protection by design and by default imperatives.

Compliance with these requirements will, however, at least in some scenarios be fraught with difficulty, as observed above. This is particularly so in the blockchain context. Indeed, these systems were invented specifically so that they can be deployed in situations devoid of interpersonal or interinstitutional trust. To this end, human intervention in the system and manipulation of the data were rendered onerous. Smart contracts can be used as a mechanism to realize that original vision. Yet, as wider use cases emerge, smart contracts are evolving to better respond to economic and legal requirements. Below, I chart these evolutions and highlight why they may also facilitate GDPR compliance.

Sophisticated smart contracts

With its origins in cypherpunk ideology, blockchains were initially designed to avert interference by outside actors, including the State. As a consequence, these systems were not fashioned having regulatory compliance in mind. Over time, new applications distanced from such ideology have appeared and it is plain that blockchains depend on law for recognition, and conversely, large-scale adoption.[132] The same rationale applies to the smart contracts deployed on these systems.

There is an ongoing trend to further sophisticate smart contracts in view of rendering them compatible with real-world requirements. Mindful of the fact that things can go awry (such as a bug in the code) or that unexpected circumstances arise the automated execution that characterizes blockchain-based smart contracts might not always be the best option. As automated execution nonetheless promises important efficiency gains and the realization of new business models, there is an ongoing wave of experimentation with mechanisms that leverage the opportunities of smart contracts and automated execution while mitigating its absolute inevitability. Two broad options emerge in this respect.

First, there are ongoing research and industry efforts to render smart contracts more sophisticated than a simple if-then relation in order to allow them to be used in complex settings. This may come to have important ancillary effects on GDPR compliance as they foresee an option of human intervention. These configurations include the use of multiple-signature verification ('MultiSig') whereby the parties need to activate the software with their respective private keys before it can

128 CNIL (n 69).

129 See further Michèle Finck, *Blockchain Regulation and Governance in Europe* (CUP 2019) Ch 4.

130 See arts5, 16 and 17 GDPR, respectively.

131 Under art 83(2)(d) GDPR due regard shall be taken of 'the degree of responsibility of the controller or processor taking into account technical and organizational measures implemented by them' when determining the fines for breach of the Regulation.

132 See further Finck (n 129).

execute.[133] In such a circumstance there is human intervention, which is moreover by the data subject and possible joint-controller herself. Two-out-of-Three MultiSig smart contracts (which require two out of three keys to authorize a transaction) would enable a purchaser of a good could transfer the price to a blockchain address that is based on three other addresses—her own, that of the seller, and that of an independent arbitrator. If the sale of goods occurs without problem, the buyer and seller could sign the transaction and release the funds. Where a problem occurs, both could use their private key to reimburse the funds to the buyer. Where a problem occurs that cannot be solved by the parties, the arbitrator would use her key to allocate funds as she sees fit.[134] It is, however, questionable whether these mechanisms could satisfy the requirements of Article 22(3) GDPR which appears to require ex post rather than ex ante human intervention.

Furthermore, there are ongoing developments of 'arbitration' mechanisms to be incorporated into smart contracts. At present, it remains an open question how systems of automated execution best deal with disputes, particularly where the smart contract forms part of a contractual setting. A solution that could be envisaged is embedding a hash of a related paper contract in the smart contract and if the smart contracts fails or has a bug, the paper contract, as interpreted by humans, would prevail. Numerous projects currently seek to integrate dispute resolution systems of this kind into smart contracts. A MultiSig could be used to halt the smart contract's execution in the event of a dispute or unforeseen consequences to call an arbitrator. The parallel legal contract could be equipped with an arbitration clause and the smart contract could integrate an arbitration library that allows to pause, resume and alter the software and which connects the smart contract with human beings.[135] A number of entities are currently developing smart contract adjudication protocols that can be used in such circumstances.[136] Other projects are working on a feature to allow to stop smart contracts (such as when an employee leaves the firm and the contract or payment needs to be halted).[137] The arbitrator can be anyone from randomly chosen crowdsourced individuals to experts appointed by the parties, and, who knows, maybe members of the judiciary in the future.

These mechanisms are primarily motivated by a desire that the execution of a smart contract reflects its parties' true intent.[138] At the same time, these developments might be a step towards GDPR compliance, constituting a form of human intervention under Article 22(3). Furthermore, where interfaces with the real world are created, these can be explored to provide information about data processing to data subjects and thus also comply with related requirements. It is worth highlighting that these processes implement something explicitly considered by the A29WP in its guidance on automated data processing. It stressed that the requirement of human intervention can be implemented through 'a link to an appeals process at the point the automated decision is delivered to the data subject, with agreed timescales for the review and a named contract point for any queries'.[139] This is precisely what these developments promise to achieve, indicating that as blockchain-based smart contracts become more sophisticated, there is a prospect of compliance-by-design by making sure that the GDPR's requirements in relation to solely automated data processing are met.

Secondly, there is the question whether in blockchain networks, a data subject can at the same be a data controller in relation to her own personal data. Decentralized computing challenges the centralized design of the GDPR whereby a user provides personal data to a controller that then processes this data independently of the data subject. Under EU data protection law, a data controller is an 'entity 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'.[140] In decentralized scenarios where many actors intervene in determining the purposes and means (the 'why and how') of data processing the binary divide between the data subject and the data controller cannot easily be upheld. The A29WP has recognized that there are scenarios in which data subjects can also be data controllers.[141] Yet, while there appears to be broad agreement that a data subject can also be a data controller in relation to the personal data of other data subjects

133 Kevin Werbach and Nicolas Cornell, 'Contracts Ex Machina' (2017) 67 Duke Law Journal, 313, 345.

134 Walter Blocher, 'The Next Big Thing: Blockchain – Bitcoin – Smart Contracts' (2016) 8 + 9 Anwaltsblatt, 612, 617.

135 See, by way of example, <http://codelegit.com/> accessed 13 August 2018.

136 See by way of example, <https://kleros.io/#> accessed 13 August 2018.

137 'This Month at OpenLaw: June 2018' (*ConsenSys Media* 16 July 2018) <https://media.consensys.net/this-month-at-openlaw-june-2018-3c71c86e468e> accessed 13 August 2018.

138 In a similar vein, auditing services for smart contracts are also emerging. See, by way of example: <https://www.sagewise.io/> accessed 13 August 2018.

139 A29WP, Guidelines on Automated Individual Decision-Making and Profiling (n 86) 32.

140 Art 4(7) GDPR.

141 Art 29 Working Party, Opinion 5/2009 on online social networking, 01189/09/EN, 5 ('the activities of a user of an SNS may not be covered by the household exemption and the user might be considered to have taken on some of the responsibilities of a data controller).

(such as in the context where information regarding multiple persons on social networks), it currently appears to be an open question whether a data subject can also be the data controller of her own personal data.

In its recent guidance on the application of the GDPR to blockchains, the French Data Protection Authority opined that where a user chooses to use blockchains for personal data processing, and has the right to add data to the chain, they are considered to determine the purposes and means of processing and are accordingly a data controller of that data.[142] Yet, the examples provided, such as that of a notary using a blockchain to process client data, underline that the Commission Nationale de l'Informatique et des Libertés ('CNIL') might only consider this to be the case where a user processes others' personal data. In a situation where the user processes her own data, the CNIL deems that that the household exemption always applies. Indeed, it argued that where a natural person trades cryptocurrency for their own account, they are not a data controller as this action is caught by Article 2 GDPR according to which the Regulation doesn't apply to personal data processing 'by a natural person in the course of a purely personal or household activity'.[143] Yet, it is questionable whether the household exemption can apply in such contexts. The Court's ruling in *Lindqvist* held that in relation to the Internet that this exemption from the scope of EU data protection law only applies to activity in the course of private or family life, 'which is clearly not the case with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people'.[144] Yet, putting personal data on the Bitcoin blockchain is essentially the same as publishing it online in terms of making it accessible to an indefinite number of people.

There is thus reason to doubt the CNIL's classification on this precise point. In the absence of the application of the household exemption, the data subject would be the data controller in respect of her own data. Indeed, in both scenarios the user determines the purposes and means of data processing (knowing that historically more emphasis has been placed on the determination of the purposes than the means to determine who is a controller under EU data protection law). Yet, it remains an open question as to whether a data subject/data controller overlap is at all possible under the GDPR knowing that its purpose is to create transparency and accountability in relation to data processing and enabling such an overlap may go counter the rationale of data subject protection. While it would give data subjects more control over their data, it may also give rise to a weakening of their rights.[145] In light of the CJEU's firm emphasis that the GDPR is a fundamental rights instrument and that it ought to be interpreted to ensure the effective and complete protection of data subjects, one may wonder whether it would accept interpretations of the data subject also being the data controller regarding data relating to them as would remove the external controller liable to protect the data subject's rights.

Conclusion

The GDPR insists that individuals should not be subjected to decisions with a significant effect on their lives, legal or otherwise, that are the result of solely automated personal data processing. While such processing can in some circumstances be designed to be compatible with EU data protection law, the GDPR imposes a number of related conditions such as that there be an option for human intervention and that the modalities of processing be explained to the data subject.

The above analysis has revealed has revealed that, while smart contracts will not automatically be lawful under Article 22 GDPR, they can be used if one of the scenarios of Article 22(2) is met, and the protective requirements of Article 22(3) are respected. In some cases, this will require a distancing from the original motivations of automated processing and the impossibility of human intervention in using these tools. Notwithstanding, such efforts would overlap with ongoing development of more sophisticated smart contracts that enable their alignment with legal postulates. This would enable the leveraging of the benefits of automated execution while also ensuring that this occurs in a manner compliant with real-world requirements and the GDPR. More generally, the observations that emerge from this research underline that the GDPR can set important innovation incentives, aiming at making sure that the advantages of automated data processing (such as increased efficiencies and resource savings) are coupled with the effective protection of fundamental rights.[146]

doi:10.1093/idpl/ipz004
Advance Access Publication 12 May 2019

142 CNIL (n 69) 2–3.

143 Art 2(2)(c) GDPR.

144 Case C-101/01 *Bodil Lindqvist* (2003) EU:C:2003:596, para 47.

145 On this tension, see further Michèle Finck, Data Subjects as Data Controllers in Decentralized Networks (draft on file with author).

146 See also A29WP, Guidelines on Automated Individual Decision-Making and Profiling (n 86) 5–6.