Smart Contracts and Smart Disclosure: Coding a GDPR Compliance Framework

Marcelo Corrales, Paulius Jurčys and George Kousiouris

Contents

Abstract This article analyses some of the main legal requirements laid down in the new European General Data Protection Regulation (GDPR) with regard to hybrid Cloud computing transformations. The GDPR imposes several restrictions on the storing, accessing, processing and transferring of personal data. This has generated some concerns with regard to its practicability and flexibility given the dynamic nature of the Internet. The current architecture and technical features of the Cloud do not allow adequate control for end-users. Therefore, in order for the Cloud adopters to be legally compliant, the design of Cloud computing architectures should include additional automated capabilities and certain *nudging* techniques to promote better choices. This article explains how to fine tune and effectively embed these legal requirements at the earlier stages of the architectural design of the computer code. This automated process focuses on Smart Contracts and Service Level Agreements (SLAs) frameworks, which include selection tools that take an information schema and a pseudo-code that follows a programming logic to process information based on that schema. The pseudo-code is

essentially the easiest way to write and design computer code, which can check automatically the legal compliance of the contractual framework. It contains a set of legal questions that have been specifically designed to urge Cloud providers to disclose relevant information and comply with the legal requirements established by the GDPR.

Keywords Smart Contracts, European General Data Protection Regulation (GDPR), Smart disclosures, Nudges, Service Level Agreements (SLAs), Unified Modeling Language (UML), Pseudo-code.

1 Introduction

Smart contracts are self-executing and autonomous computer protocols that facilitate the performance and execution of agreements between two or more parties. The advantages of smart contracts are numerous. They can provide better security performance than traditional contract law and reduce transaction costs associated with the negotiation, verification and enforcement of agreements.[1]

They are encoded in such a way that the correct execution is guaranteed by the blockchain.[2] The blockchain is essentially a distributed ledger that can be configured to be accessible publicly or privately and the technology guarantees the transaction history.[3] This blockchain-based smart contract technology allows the involved parties to transfer, receive and store value or information through a distributed peer-to-peer computer network.[4] Decisions are typically based on a majority vote while variations exist in which accessors of information may have only partial access to a selected subset of the data (permissioned blockchains).[5]

In other words, each transaction is distributed across the entire network and is stored in a block only when the rest of the network approves the validity of the transaction. This process is based on past events taking into account the previous block.[6] Each block holds a unique fingerprint built on cryptographic hash code techniques similar to those used in the creation of digital certificates and electronic signatures to secure authentication.[7] Furthermore, a transaction history is maintained and can be accessed in order to check the sequence of events up to this point in time

The main purpose of smart contracts is to automate obligations, which are held as "code." As Lawrence Lessig ably stated: "code is law."[8] Code is essentially the set of rules or instructions that structure the Internet. That is, the hardware and software applications that "make" the Internet architecture as it is.[9] Denise Carusso has also powerfully stated:

---

[1] Carnevale (2017), pp. 64-65; Wattenhofer (2016), p. 88.
[2] Kost de Sevres (2016); Wattenhofer (2016), p. 88.
[3] Wattenhofer (2016), p. 88; Swan (2015), p. 16.
[4] See e.g., generally, Morabito (2017); Swan (2015).
[5] Varshney (2017).
[6] Kost de Sevres (2016).
[7] Mougayar (2015).
[8] Lessig (2006), p. 1.
[9] Post (2009), p. 129.

> "It is still true today that software — written by a team of sleep-deprived programmers in some fusty cubicle — is the code that lays down the absolute law by which we live our lives. We are not free to change that code; our choice is to love it or leave it."[10]

One of the main challenges of smart contracts will be to embed the laws of the physical world into the digital code. The crucial question is how to translate these technical options into an agreement.[11] This is the reason why lawyers can (and should) learn how to code. Coding is essentially just a range of agnostic problem-solving techniques and tools.[12]

Thus, the best way to start coding is through "pseudo-code." Pseudo-code is the best way to write and design computer software *before* it is coded. In Myler's view, pseudo-code is "a simple, structured representation of a program sequence or algorithm that is not intended to be run on a machine."[13] In other words, it is the outline of a program without using any specific programming language.[14]

To put it another way, the pseudo-code describes how the designer would implement an algorithm without getting distracted by the syntactical language details.[15] It is essentially a generic text containing some keywords that provide specific instructions to write the programming language itself. This way the pseudo-code can then easily be translated into the specific source code[16] and thus implemented both in the preliminary and detailed architectural design stages.[17]

Smart contracts could be developed on a pseudo-code based on "If" and "Then" statements. The aim of this article is, therefore, to present an example of a pseudo-code template, which includes the disclosure of relevant legal (and technical) information using *smart disclosures* as prime nudging techniques. This will prompt Cloud computing providers to effect the necessary changes in their SLAs and underlying software in order to make the processing of personal data compliant with the new European General Data Protection Regulation (GDPR).[18]

This article is divided in 9 sections. After this introduction, section 2 highlights some of the key components and changes proposed by the GDPR. Section 3 explains the new challenges of managing Smart Contract SLAs in Cloud computing transformations. Section 4 adopts the behavioral law and economics approach to *nudge* and positively influence decision-making in Cloud computing architectures. Section 5 focuses on *smart*

---

10 Lessig (2001), p. 283.
11 Asharaf and Adarsh (2017), p. 50.
12 Hogan (2017).
13 Myler (1998), p. 37.
14 Kamthane and Kamal (2012), pp. 79-80.
15 Ford (2015), p. 163; ISRD Group (2007), p. 192; ITL Education Solutions (2006), p. 222.
16 Brooks (1997), p. 27.
17 Agarwal, Tayal and Gupta (2010), p. 130.
18 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). While the Regulation entered into force on 24 May 2016, it shall apply to all EU Member States from 25 May 2018. See European Commission, Reform of EU Data Protection Rules http://ec.europa.eu/justice/data-protection/reform/index_en.htm Accessed 10 October 2016

disclosures as they are considered to be one of the most powerful nudging techniques. Section 6 follows Nudge Theory and proposes the implementation of embedded legal and technical questions in order to disclose relevant information as part of a Unified Modeling Language (UML) schema. Section 7 elaborates on the idea of a pseudo-code, which is also an integral component of the Smart Contract SLA framework. Section 8 presents a set of legal and technical questions — which is necessary for the elaboration of the pseudo-code — and explains in detail the programming logic that have been carefully crafted to comply with the new provisions enshrined in the GDPR. Finally, section 9 concludes.

2 Key areas to consider with regard to the GDPR

The advent of Cloud computing, Big Data and Internet of Things (IoT) poses great challenges concerning the processing of personal data especially in hybrid Cloud scenarios. This section presents some of the main legal requirements that need to be taken into account in light of the new GDPR. While the GDPR proscribes some new rights to create more transparency and empower data subjects, it has also sparked criticisms with regard to the increased burden and responsibilities imposed on data controllers and data processors.

Some of these limitations may fall foul of the current Big Data and IoT movement, in particular if one looks at this problem from a global perspective. This means that we need a whole new contractual framework. Therefore, one of the main objectives of this article is how to translate and effectively embed those new legal requirements (sometimes seen as constraints) in the computer code of Cloud architectures.

The GDPR was adopted on 27 April 2016 and after a two-year transition period it will come into force on 25 May 2018. The GDPR replaced the previous European Data Protection Directive[19] and was designed to strengthen and unify data protection and privacy for all European Union (EU) citizens and to empower individuals by granting them more control and certainty over their data when using Internet services.[20]

The GDPR has been generally welcomed for updating some of the rules of the previous data protection regime. However, it has also created concerns among legal scholars and privacy associations. The most significant changes that triggered heated discussions, which deserve a closer attention in the context of this article can be summarized as follows:

i. *International Data Transfers:* The GDPR imposes more stringent rules for the transfer of personal data to third countries and international organizations outside the EU. This change was designed to ensure an adequate level of protection in a globally connected world;[21]
ii. *Extra-Territorial Scope:* The GDPR expands its territorial scope of protection

[19] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[20] See, e.g., Mc Nealy and Flowers (2015), p. 199; Gjermundrød, Dionysiou and Costa (2016), p. 4.
[21] Art. 46 GDPR; Voigt and von dem Bussche (2017), p. 120.

(extra-territorial applicability) to data controllers and processors established in the EU and *outside* of the EU territory with regard to the processing of personal data of European citizens;[22]

iii. *Consent:* The GDPR strengthens the definition of consent, meaning that consent must be concise, unambiguous, clear and freely given. Companies will no longer be able to use long terms and conditions full of legalese;[23]

iv. *Breach Notification:* Data breach notifications are mandatory. Data controllers must notify the breach immediately (within 72 hours) to their supervisory authority, whereas data processors must report the breach to the controllers;[24]

v. *Access Rights:* Data subjects have more rights to get access and control regarding their data. This allows them the right to request the data controller whether personal data concerning them is being processed, where and for what purpose;[25]

vi. *Right to be Forgotten (data erasure):* This right endows data subjects to have the controller delete their personal data and stop further processing and dissemination of data from third parties;[26]

vii. *Data Portability:* The GDPR creates a new right to data portability. This right allows data subjects to receive their personal data concerning them — which they have previously submitted to the data controller — in a "structured, commonly used and machine-readable format," and to send those data to another controller;[27]

viii. *Privacy by Design and by Default:* The Privacy by Design (PbD) approach was first introduced by the Information and Privacy Commissioner of Ontario,[28] and has existed as a general concept ever since. The PbD entails the notion of embedding privacy (and data protection) requirements directly into the architecture design of information technologies and related systems. However, the GDPR introduces, for the first time, the PbD (and Privacy by Default) as a legal obligation. Data controllers and processors must adopt this approach by default, making an explicit reference to "data minimization"[29] and the possible use of "pseudonymization."[30]

---

[22] See Art. 4 (1) (c) of the GDPR; Svantesson (2013), p. 89; Hijmans (2016), p. 497.
[23] See Recital 43, Art. 7 (4) of the GDPR; Wisman (2017), p. 357.
[24] See Art. 33 of the GDPR; Müthlein (2017), p. 78.
[25] See Arts. 12-14 of the GDPR; Quelle (2016), p. 143.
[26] See Art. 17 of the GDPR; Sobkow (2017), p. 36.
[27] See Art. 20 of the GDPR; see also Article 29 Data Protection Working Party, Guidelines on the right to data portability. Adopted on 13 December 2016. As last revised and adopted on 5 April 2017; see also Fosch Villaronga (2018), p. 232.
[28] Cavoukian (2015), pp. 293 et seq.; see also Information and Privacy Commissioner of Ontario https://www.ipc.on.ca/?redirect=https://www.ipc.on.ca/ Accessed 10 October 2017.
[29] See Art. 5(1)(c) of the GDPR; Lynskey (2015), p. 206; Thouvenin (2017), p. 218.
[30] See Art. 25(1) of the GDPR; see also D'Acquisto et al. (2015); Voigt and von dem Bussche (2017), p. 62.

3 Smart SLAs in the Cloud

The Cloud is an emerging trend that can be broadly defined as "an architecture by which data and applications reside in cyberspace, allowing users to access them through any web connected device."[31] The Cloud changed the way services are managed today offering a variety of resources for businesses[32] and scientific institutions.[33] The main reason for this shift is that IT resources in the Cloud are no longer stored on end-user personal devices, but accessed through a distributed network.[34]

The Cloud allows consumers to operate a broad gamut of applications ranging from email and web-based spreadsheet services to more robust and reliable business software.[35] It touches upon almost every corner of our society. Evidence of the ubiquitous nature of the Cloud abounds in our daily life activity during time spent on the Internet. The following are best examples of Cloud computing services: webmail services such as Gmail or Yahoo; blogging or social networking sites such as Twitter, Facebook or LinkedIn; picture sharing platforms such as Instagram; or even rating sites such as Tripadvisor.[36]

The Cloud is, however, much more than this. It is an Internet-based computing network that provides services enabling individuals and companies to jointly access a shared pool of resources and information.[37] Its benefits have contributed to improve all aspects of the society. From a service provider perspective, the Cloud optimizes resources. From a customer standpoint, the Cloud reduces costs in terms of hardware, software and other services.[38]

The main problem is that these services have different SLAs tied to it and this is often the last thing a customer of Cloud services will review. SLAs are essentially contracts that resemble those outsourcing agreements, web hosting services[39] and application service agreements[40] found on the Internet. They provide similar terms and conditions that the involved parties need to fulfill. The main difference is that in the traditional form of outsourcing agreements the customer deals directly with the service provider, knowing exactly the type of service and where the IT infrastructure is located.[41]

SLAs are legally binding contracts used to guarantee the quality of service (QoS) and fulfill the expectations between the parties at both organizational and operational levels. These include the appropriate sanctions and penalties if the services are not delivered according to the terms and conditions. Their structure is similar to software license agreements, however, with regard to their subject matter they fall under the same

---

[31] Horrigan (2008).
[32] Millham (2012), p. 2.
[33] Balasubramanyam (2013), p. 102.
[34] Kasemsap (2015),
[35] See, e.g., IBM cloud computing, Cisco cloud computing, Microsoft Azure, Rackspace and Amazon Web Services (AWS).
[36] Naughton and Dredge (2011).
[37] Moskowitz (2017), p. 59.
[38] Hossain (2013), p. 14.
[39] See, e.g., King and Squillante (2005), pp. 195 et seq.
[40] See, e.g., Harney (2002), p. 126.
[41] See, e.g., generally, Kimball (2010).

category of outsourcing and hosting agreements.[42] SLAs in the Cloud are different as they depend entirely on customer's demand.[43] The Cloud has brought an increased number of intermediaries and different types of Cloud providers to fulfill the QoS.

Therefore, the main idea of this article is to propose a more flexible template, which is also in compliance with the GDPR. A Smart Contract SLA should provide a sound legal basis for the contracting parties and should follow the PbD approach. If this is not properly developed at early stages of the architectural design of the computer code — at least for functions that select suitable Cloud services from an available pool — it may cause harm and unexpected side effects to the involved parties.

For large buyers of Cloud, certain terms of the Smart SLA may be negotiable depending on the Cloud provider and how interested they are in keeping the company as a client.[44] For small buyers, however, these terms are usually drafted on a "take it or leave it" basis. Not to mention the "legalese" complexities of the terms of service that a customer must grapple with. The importance and difficulty of this has been examined by the House of Commons Science and Technology Committee in the UK describing them as "more complex than Shakespeare."[45]

They found out that consumers generally just sign up the agreements without knowing exactly what these terms really mean.[46] Evidence of this is the Article 29 Data Protection Working Party recommendation to Google to clarify its privacy policy so as to avoid "indistinct language."[47] Another example of this problem is revealed in the recent study of Facebook's Data Policy, which concluded that it was unclear to which extent user's data is shared with other companies and third party partners.[48]

4 Choice Architectures, Nudges and Legal Compliance

Following the foregoing discussion, the overarching idea in this article is to alter the choice architecture of computer software systems and frame key legal questions that can automatically influence certain positive behavior and lead to legal compliance. The end goal is thus not to "hardcode" open legal norms, but to *nudge* cloud providers in achieving a greater level of compliance taking into account those legal rules.[49]

According to Olislaegers, compliance software consists of primarily "hardcoded legal knowledge on the one hand, and, when the law cannot be hardcoded, of nudging mechanisms on the other hand."[50] Therefore certain nudging techniques can help business comply with the legal requirements of e.g., the GDPR.

---

[42] Bragg (2006), p. 49; Svirkas (2004), pp. 96 et seq.
[43] Carstensen, Morgenthal and Golden (2012), p. 244.
[44] Griggs (2013).
[45] Anderson (2015), p. 159.
[46] Anderson (2015), p. 159.
[47] Anderson (2015), p. 159; see also, letter from the Article 29 Data Protection Working Party to Google on Google Privacy Policy (Appendix: List of Possible Compliance Measures. Ref. Ares (2014) 3113072).
[48] Anderson (2015), p. 159; see also Van Alsenoy et al. (2015).
[49] See, e.g., Olislaegers (2012), p. 80.
[50] See, e.g., Olislaegers (2012), p. 80.

Over the past decades, behavioral economics has been a growing force in various fields of social sciences including many important legal domains.[51] Behavioral law and economics blends the traditional economic analysis of law and places greater emphasis on behavioral psychology. Its main premises stem from the innate human propensity to "err" in making decisions focusing on the understanding of human behavior. This approach may help us to better understand the difficulties of decision-making and find a better solution to improve the legal environment.[52]

The idea of this integrated normative framework was popularized by Richard Thaler and Cass Sunstein,[53] in their book *Nudge: Improving Decisions about Health, Wealth and Happiness*.[54] Their main argument is that improved choices and information disclosure could prevent individuals from making mistakes, enabling them to be better off.[55] This includes the ideas behind Nudge Theory. The definition of a nudge is "any aspect of the overall choice architecture that alters people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives."[56] In other words, this refers to "every small feature in the environment that attracts our attention and influences the decisions that we make."[57]

The person who manipulates such environment is called a "choice architect." By and large, choice architects arrange the context that affects individual's decision-making.[58] Nudges are therefore those small changes in the choice architecture.[59] To count as a nudge, this intervention must be easy, inexpensive,[60] and most importantly, it must respect people's autonomy without coercing them to comply.[61] A well-designed architecture is only useful if it helps the involved parties to make better decisions, which is also necessary for developing a consistent and consolidated contractual framework.

Therefore, the very center idea of this research study is to encourage choice architects to transform the online environment and improve the choices that we have. This can be achieved by making small changes in the overall architecture design of Smart SLAs. Thaler and Sunstein defend the thesis that small changes in choice architectures are indispensable to improve individual's welfare. This notion of choice architecture embraces various dimensions. Examples of this abound in different fields, which show how making small changes can make a big difference such as: one-sized or double-sized printing, automatic enrollment of organ donation or pension funds, or customized reminders deadlines to qualify for a student loan.[62]

By way of illustration consider the example related to the choice of post-mortem organ donation.[63] Two widely accepted default systems exist: a) opt-out system, whereby

---

51 See, e.g., generally, Jolls (2010); Diamond and Vartiainen (2007) (eds).
52 See, e.g., generally, Zamir and Teichman (2014) (eds).
53 Sunstein (2000) (ed); Sunstein (2014b).
54 See Thaler and Sunstein (2009);
55 Corrales and Jurčys (2016), p. 533.
56 Briggs, Jeske and Coventry (), p. 117.
57 Willis (2015).
58 Bernheim et al. (2015), p. 35.
59 Whyte et al. (2015), p. 171.
60 Cwalina, Falkowski and Newman (2015), p. 78.
61 Schweizer (2016), p. 111.
62 Corrales and Jurčys (2016), p. 533.
63 Ben-Porath (2010), p. 11.

consent is automatically assumed; b) opt-in system, which requires explicit consent from the deceased.[64] In the first system this means that you are a donor by default, whereas in the second system this means that you need an active choice.[65] The procedure differs from country to country.

For example, in some areas of the U.S., this requires the deceased having previously enrolled in a state registry. In other countries, such as Japan and most European countries, however, individuals are given this choice when they get or renew their driving license. In this case they can check a box as an opt-in or opt-out rule.[66] In countries with an opt-in default system — such as Denmark and the Netherlands — the percentage of organ donation is very low[67] in comparison to opt-out systems — such as Spain, Austria, France, Hungary, Poland and Portugal.[68] The reason for this is that people tend to prefer options that do not require mental effort (i.e., deliberation costs).[69]

Another meaningful example for embedding nudging techniques in the design of (software) architectures is the default settings of printer machines. Double-sized or single-sized printing might require users to click a button in the printer "preferences" or even the "advanced properties" settings. People use a lot more papers with single-sized prints.[70] However, this can also be selected as a standard double-sized default rule, thereby being more environmentally friendly and more cost-effective for the society.

A few years ago, an empirical research study carried out at Rutgers University in the U.S. adopted a double-sized default. The study revealed a significant reduction of 44% in paper consumption during the first 3 years. This is the equivalent of 55 million paper sheets, which amounts to 4,650 trees. This shows how relatively small changes embedded in the architecture design of computer software can have an immediate effect and produce a large impact in the long run.[71]

5 Smart Disclosures in Automated Smart Contracts

According to the Behavioral Law and Economics literature one of most powerful nudging techniques are *information disclosures*. Information disclosure is about giving people just the right piece of information that may influence their decisions in one way or another.[72] The message contained in the "information nudge" may activate a certain schema in

---

[64] Heshmat (2015), p. 243; Detels and Gulliford (2015), p. 782.
[65] Detels and Gulliford (2015), p. 782.
[66] Detels and Gulliford (2015), pp. 23 and 108; See also John (2013), p. 104; Quigley and Stokes (2015), p. 64; Thaler (2009); Hamilton and Zufiaurre (2014), p. 18.
[67] European Commission (2014), Journalist Workshop on Organ Donation and Transplantation: Recent Facts & Figures. Available at: http://ec.europa.eu/health/sites/health/files/blood_tissues_organs/docs/ev_20141126_factsfigures_en.pdf Accessed 13 April 2017.
[68] Leitzel (2015), p. 137.
[69] Cahn (2013), p. 148.
[70] Sunstein (), p.
[71] Sunstein (2015b), p. 26.
[72] Lindahl and Stikvoort (2015), p. 45.

people's brains. One concept, which is part of such schema, can trigger other concepts in the same schema.[73]

For example, "eco-labeling" schemes often inform consumers about the sustainability of the product.[74] One way this type of information disclosure may function as a nudge is when the individual has a sort of "self-identity" related to environmental issues. The information contained in the eco-label may activate a thought that reminds the person of his or her eco-friendly self-identity. Applying eco-labeling schemes therefore help consumers to better understand the options they have and to make informed decisions. This can also raise a wider eco-friendly awareness among consumers and promote environmental responsibility among producers.[75]

For the purposes of smart contracts, we need to adopt "smart disclosure" strategies to provide objective information and allow end-users to quickly assess the attributes and legal compliance of Cloud providers. The idea of "smart disclosure" has been a recurrent subject over last years, which is kindling interest in various fields of law as a measure for improving consumer choices.[76]

The term "smart disclosure" in this sense refers to "the timely release of complex information and data in *standardize*, *machine readable formats* [emphasis added] in ways that enable consumers to make more informed decisions."[77] Smart disclosures are adaptive, interoperable and innovative to markets.[78] The role of smart disclosures should be to provide more alternatives the consumer did not consider before or remind them to take something into account but they may have forgotten.[79]

Examples of smart disclosures exist across various regulatory fields such as: product safety, finance, energy regulation, employment law, environmental law and health law.[80] One of the most powerful smart disclosure techniques is when data on products or services (including algorithms) is merged with personal data (such as customer location data) into "choice engines" (such as mobile applications in the Cloud) that allow end-users to make better contractual decisions. There are four general categories where smart disclosure applies as follows:[81]

i) *When government discloses information about products or services:* For example, when the U.S. Health Department releases hospital quality ratings, or when the Security and Exchange Commission discloses public financial data in machine-readable format.[82]
ii) *When government discloses personal data about citizens:* For example, when the Internal Revenue Service (IRS) provides citizens with online access to their electronic track records.[83]

---

73 Lindahl and Stikvoort (2015), pp. 28-30.
74 Lindahl and Stikvoort (2015), pp. 28-30.
75 Lindahl and Stikvoort (2015), pp. 28-30.
76 Tereszkiewicz (2016), p. 177; Bar-Gill (2012), p. 41.
77 Sunstein (2014a), p. 98.
78 Marc et al. (2015), p. 529.
79 Lindahl and Stikvoort (2015), pp. 28-30.
80 See, e.g., generally, Ho (2012), pp. 574-688.
81 Howard (2012).
82 Howard (2012).
83 Howard (2012).

iii) *When a private company discloses information about products or services in machine-readable formats:* For instance, when a company launches a website with relevant information and applications that can empower consumers to calculate their taxes and improve their finances.[84]

iv) *When a private company releases personal information about usage to a consumer:* For example, when a power company provides utility customers with user-friendly and secure access to its energy usage data through e.g., the "Green Button."[85]

Currently, one of the most promising regulatory strategies consists of "targeted disclosure." This urges choice architects to disclose simplified information at the time when consumers have to make decisions. Restaurant sanitation grading is a good example that has empowered consumers and incentivized restaurant owners to improve their sanitation conditions in order to reduce risks for foodborne illness (such as salmonella) caused by bacteria, parasites, toxins and viruses.[86]

A simple notice displayed at the restaurant entrance, which summarizes sanitation information with a certification ranking system ("A", "B", or "C") can reduce the information gap and nudge the involved parties along.[87] In this sense, targeted disclosures are a direct response to the so-called "behavioral market failures" and provides a justification for the government to intervene.[88] This improves not only transparency but allows consumers to compare the choices that they have.[89]

In other words, these kinds of smart disclosures help consumers to select restaurants based on health risks, which in turn urges restaurants to clean up.[90] The Mayor of New York City Michael Bloomberg introduced restaurant inspection and grading system in 2010 arguing that this helped to improve food safety practices and reduce foodborne illness outbreaks. [91] Furthermore, this information (about specific restaurant grading) is available online as open data and can be retrieved and portrayed to end-users through mobile applications. Archon Fung et al. have also documented how these embedded smart disclosures have played a significant role in improving restaurant hygiene in the city of Los Angeles.[92]

Following these theoretical and empirical examples, one of the main objectives of this study is about the importance of choosing the right institutions and mechanisms when addressing such behavioral market failures in the context of smart contracts. The sections below propose a unique way of urging Cloud providers to disclose relevant information, which could be pursued to address the emerging challenges in the Cloud computing market.

---

[84] Howard (2012); see, e.g., http://www.hellowallet.com
[85] Howard (2012); see, e.g., http://www.greenbuttondata.org
[86] Ho (2012), pp. 574-575.
[87] Ho (2012), pp. 574-575.
[88] For more details on "behavioral market failures" and default rules as nudging strategies see, e.g., Sunstein (2015b), pp. 206 and 218.
[89] Busch (2016), p. 231. According to Daniel Ho, however, this grading system contains serious flaws and does not guarantee 100% cleanliness down the road. See Ho (2012), pp. 574-688.
[90] Ho (2012), pp. 574-575.
[91] Grynbaum and Taylor (2012).
[92] Fung, Graham and Weil (2007), pp. 44, 50-51, 59-62, 68, 82-83, 120, 179.

6 A Unified Modeling Language for Checking Legal Compliance

This section presents the elaboration and capabilities of a Unified Model Language (UML) as an extension to the overall contractual framework of Cloud software architectures. The UML-description includes a selection tool that exports their options through a Graphical User Interface (GUI). This will allow end-users to select the most favorable options they have.

UML is a standardized "general-purpose language for modeling object-oriented systems,"[93] which allows software architects to "specify, visualize, build and document the artifacts of software-intensive systems."[94] The idea behind such a language is to model software systems before its construction, and simultaneously, to automate and improve the quality process. Thus, reducing transaction costs and shortening time to market.[95]

Considering that UML language is very specific and formal, it became one of the most common standard modeling languages that facilitates communication and reduces uncertainty between analysts and people.[96] Just like architects have their own standards for representing their technical graphs and designs, software developers have also developed a unified and universally accepted modeling language.[97] Therefore, UML is specially adapted to support the architectural design of software systems.[98] With respect to end-user input and interface, this could be done via web forms, which can directly export schema files and create the necessary options. There are many tools for this that can enable a more simple and user-friendly interface and design.[99]

The UML-description schema will aid in checking the legal compliance, which is necessary for choosing a Cloud provider and outsourcing data in an automated fashion. This can serve as the basis for expanding the scope of SLAs and making strategic choices of Cloud providers a global reality. This idea was taken from the ARTIST project[100] and can be implemented as an adjunct to any SLA framework for reducing the information gap and improving the understanding between the involved parties.

The ARTIST project comprises a certification model with a set of legal questions that certifies whether the migrated software is compliant with the legal requirements or not. Similar to the example of the restaurant sanitation grading system explained in the previous section, the major goal of the ARTIST certification model is to elicit answers to a set of questions that can then be translated into a rating system for the used software

---

93 Overgaard (1999), p. 99.
94 Debbabi et al. (2010), p. 37.
95 Debbabi et al. (2010), p. 37.
96 Patel (2005), p. 206.
97 Galis (2000), p. 87.
98 Muresan (2009), p. 233.
99 See, e.g., generally, Hennicher and Koch (2001), pp. 158-172.
100 Advanced Software-based Service Provisioning and Migration of Legacy Software (ARTIST). This project was partially funded by the European Commission under the Seventh (FP7 - 2007-2013) Framework Program for Research and Technological Development. For more details about the ARTIST project, see: http://www.artist-project.eu/content/r12-certification-model#sthash.zpJSBZ9t.dpuf. Accessed 18 May 2016.

(such as Gold, Silver and Bronze).[101] This component is fundamental for increasing end-user's trust in software applications taking into account certain parameters (categories) to be evaluated.[102]

In the context of this article, however, the conclusion would be more straightforward and it would be of a "True" and "False" nature. Thus, it is either legally compliant or not. The questions are set as closed and pre-defined options since there are in principle only two possible responses: "Yes" or "No". "Yes" means that the answer to the question is either "Yes" or "Configurable in the SLA." The latter answer will allow Cloud service providers to effect any necessary changes within their own SLAs.

This is where framing questions to disclose information based on Nudge Theory comes to the fore. These questions could effectively be embedded in a coordinated fashion at different layers, especially if one follows a programming logic approach according to which one can check automatically the legal compliance. These questions would aim at nudging Cloud providers to disclose relevant information urging them to make further modifications in the SLAs and its underlying software.

Questions vary depending on the nature of the Cloud services required and the legal needs of the involved parties. They were designed to answer a broad range of legal issues in an automated fashion based on — primarily — the legal requirements of the GDPR. Depending on the nature of the service, questions range from privacy, data protection and data security. No free text is allowed, but pre-defined selections. This will enable the writing of the computer code, which has the ability to internally process the answers and produce an automatic result.

In this way, a pseudo-code has been created in order to communicate the legal requirements based on the requests made by the concerned parties. If the service provider cannot meet these legal requirements, end-users should be able to make a decision whether they still want to use the software application. If not, they should be able to migrate and choose another service. The section below explains in more detail the features of the pseudo-code.

7 Nudging Cloud Providers Through a Pseudo-code

As hinted above in the introduction of this article, the pseudo-code describes how the designer would implement an algorithm without getting distracted by the syntactical language details.[103] The pseudo-code is essentially a generic text containing some keywords that provide specific instructions to write the programming language itself. This way the pseudo-code can then easily be translated into the specific source code[104] and thus implemented both in the preliminary and detailed architectural design stages.[105]

---

[101] ARTIST R12 Certification Model. Available at: http://www.artist-project.eu/content/r12-certification-model. Accessed 10 December 2016.

[102] ARTIST R12 Certification Model. Available at: http://www.artist-project.eu/content/r12-certification-model. Accessed 10 December 2016.

[103] Ford (2015), p. 163; ISRD Group (2007), p. 192; ITL Education Solutions (2006), p. 222.

[104] Brooks (1997), p. 27.

[105] Agarwal, Tayal and Gupta (2010), p. 130.

In other words, it is like a flowchart, but without the graphics.[106] In this context the prefix "pseudo" means that it is not the actual source code, but the synthetic expression of it.[107]

During the elaboration of the pseudo-code, the software architect uses short English language words that follow a structural logical order. Phrases such as: "If-Then-Else, and End" are keywords used to design the structure of the programming language. Hyphens are used to link keywords to describe the control flow, while other English words are used to describe the processing actions.[108] For example: If A=B, Then C=A, Else C=D. The best way to explain a pseudo-code in simple terms is by describing step-by-step the process of making a cup of coffee as follows:

PROGRAM (name): "Make a cup of coffee"

i. Fetch and organize all the necessary utensils and ingredients.
ii. Plug the coffee machine.
iii. Put the filter inside the coffee machine.
iv. Put coffee grains inside the filter of the coffee machine.
v. Fill the coffee machine with water.
vi. Wait 10 minutes until coffee is ready.
vii. Get a mug.
viii. Fill the mug with coffee.
ix. Add milk and/or sugar.
x. Serve.

END

As shown in the example above, the first step when designing a program is to choose a name. In this case the name is "Make a cup of coffee." Then, one needs to follow the instructions step by step until the "end" point. Each of these steps is called a "sequence." Now, the question is what happens if one has to make a choice in step "ix" between adding milk and/or sugar? The answer is to include a "selection switch" in the sequence. For instance, IF (sugar is needed), THEN add sugar, ELSE do not add sugar.[109]

In the context of this article we want to write the pseudo-code for a computer software that can nudge Cloud service providers to improve their choice architectures and check automatically the legal compliance of their SLAs. Therefore, a good name for the program would be: "Check Legal Compliance." The pseudo-code will then follow the same general conditional formula IF (condition to be checked) THEN (if condition is true) ELSE (if condition is false) ENDIF, as set out in the "Make a cup of coffee" example above.

All in all, the pseudo-code is a good tool especially for lawyers as it takes less time and effort than developing any other programming tool. It also allows more flexibility since there are no strict rules to come up with the pseudo-logic. As a rule of thumb, the simpler the statements, the better.[110] This process would also enable feeding the described

---

[106] Myler (1998), p. 37.
[107] Agarwal, Tayal and Gupta (2010), p. 130.
[108] Agarwal, Tayal and Gupta (2010), p. 130.
[109] Gries and Gries (2005), pp. 84-86; Barlow and Barnett (1998), p. 99.
[110] Myler (1998), p. 37.

pseudo-code to software developers in a more direct manner for the formal implementation of the respective code. This way interdisciplinary endeavors requiring collaboration between legal and computer science professionals could be made significantly more clear and unambiguous.

8 Legal Questions for the Elaboration of a Pseudo-Code: Check Legal Compliance

In order to extract a conclusion from the pseudo-code, one should elaborate first a list of questions related to specific legal issues. A table of all relevant legal questions has been included in Table 1 below. The table includes a set of 15 questions related to a range of legal and technical issues including, privacy, data protection and data security. This is mainly relevant for two reasons. First, it is important to cover a wide range of legal and technical issues. Second, in some cases, partial aspects of one question are related and follow the previous questions.

This set of questions has been customized and carefully crafted to include some of the main legal issues related to the new GDPR requirements as explained above in section 2. It is important to note, however, that these questions are not exclusively related to the SLA specifications, but also to the general process or design of an application/usage of the underlying resources.

1) (L001) Does your SaaS application deal with sensitive/personal data?
2) (L002) Does your SaaS application support native encryption/protection of the data and authentication?
3) (L003) Does your SaaS application give the choice of EU-based data storage location?
4) (L004) Is your SaaS application dynamically configured for using IaaS/PaaS services?
5) (L005) Are the data or metadata "ownership" rights clearly defined and clarified in the contract/SLA?
6) (L006) Do you offer notifications in case you change the terms and conditions?
7) (L007) Do you offer notifications in case your underlying PaaS/IaaS provider changes the terms and conditions?
8) (L008) Do you offer the ability to the end-users to virtually be under more control over their own data ensuring data portability (e.g., migration, extraction and reuse of their data) and interoperability within the Cloud?
9) (L009) Do you offer the ability to the end-users the right to delete/eliminate their data (so-called "Right to be Forgotten") in the original used service?
10) (L010) Does your underlying PaaS/IaaS provider use Standard Contractual Clauses (SCCs) with you and other parties?
11) (L011) Has your underlying PaaS/IaaS provider been certified for their Binding Corporate Rules (BCR) clauses by a EU DPA?
12) (L012) Do you take measures to prevent data loss (regular backups, replication, etc.)?
13) (L013) Are you using your own resources to run your application?

14) (L014) Do you restrict access of data (without prior consent of the data subject) to third parties for specific purposes?
15) (L015) Is there any auditing mechanism through which the data subject can be informed (e.g., in case of data breach or data access) about disclosure of their data and when?

Table 1 Legal questions for the extraction of the pseudo-code

Following the legal analysis and the programming code developed in the OPTIMIS toolkit[111] and ARTIST project, a pseudo-code has been created as depicted below in Table 2. The pseudo-code follows a logical order where a number of values have been assigned to each legal question. For example, question 1 has been substituted for (L001), question 2 for (L002), question 3 for (L003), etc. Then, the pseudo-code has been broken down in categories in a logical linear manner, there is a specific category assigned to the legal compliance. The result of a legal analysis has been made explicitly clear and has a binary form answering the questions "Yes" or "No" (i.e., "legally compliant" or "not legally compliant"). Table 2 below shows a fragment of the pseudo-code.

PROGRAM: "Check Legal Compliance"

```
//compliance refers primarily to the GDPR
//YES means that the answer to the question is either YES or Configurable in the
//SLA
// The symbol "//" implies a comment line, meaning the text after // does not
//affect execution, it is only used to explain the specific program line and enhance
//code readability
// The word " LEGAL_COMPLIANCE" is a variable, meaning a position in the
//memory structure of the computing system that holds the value (outcome of the
//analysis: true or false for being legally compliant)
// The symbol "=" is an assignment operator, meaning that the value at the right of
//the "=" is stored in the memory position that is indicated by the (variable) name
//on the left of the "="
//The symbol "==" indicates equality between the elements (variables and/or
//values) to the left and right of the symbol
//The word "Return LEGAL_COMPLIANCE" means stop executing and return
//the value of the variable LEGAL_COMPLIANCE at that point

LEGAL_COMPLIANCE=True;

If (L001==YES){
        If ((L002==NO)OR(L005==NO)OR(L006==NO)OR(L007==NO)
        OR(L008==NO)OR(L012==NO)){
                LEGAL_COMPLIANCE=False;
                Return LEGAL_COMPLIANCE; //stop legal analysis,
                final conclusion is reached
```

[111] *See:* CHULANI, I., et al., 2012, *op. cit.*

```
}

If (L003==NO){ //if not based in the EU, you need to be certified for BCR for EU
usage
        If (L011==NO){
                LEGAL_COMPLIANCE=False;
                Return LEGAL_COMPLIANCE; //stop legal analysis, final
                conclusion is reached
}

If (L003==YES){// if based in the EU,
            If (L009==YES){ //and you can offer the possibility to delete data
                        //do nothing, legal compliance has been set to true before
                                    }
                        }else{
                                    LEGAL_COMPLIANCE=False;
                                    Return LEGAL_COMPLIANCE; //stop legal
                                    analysis, final conclusion is reached
                        }
            }
}

If (L001==YES){ //if your SaaS application deals with sensitive/personal data
            If (L003==YES){// if based in the EU,
                If (L014=YES){ //if you restrict access of data to third parties
                        //do nothing, legal compliance has been set to true before
                        }
        }else{
                LEGAL_COMPLIANCE=False;
                Return LEGAL_COMPLIANCE; //stop legal analysis, final
                conclusion is reached
        }

}
If (L001==YES){ //if your SaaS application deals with sensitive/personal data
        If (L015=YES){ //if there is any auditing mechanism about data
disclosures
                //do nothing, legal compliance has been set to true before
                        }
        }else{
                LEGAL_COMPLIANCE=False;
                Return LEGAL_COMPLIANCE; //stop legal analysis, final
                conclusion is reached
        }

}
```

```
Return LEGAL COMPLIANCE;

//continuous iteration section

If ((L004==YES)OR(L013==YES) { // Reiterate the code below continuously
        while (true){
                If (L003==NO { //you need to be either in white list with SCC or
                wherever with BCR
                        If ((Countries in White
                        List==true)AND((L010==YES))OR(L011==YES){
                        //do nothing since legal compliance is already set to True
                } else {
                        LEGAL_COMPLIANCE=False;
                        Return LEGAL_COMPLIANCE;
                }
        }
}
```

Table 2 Pseudo-code: Check Legal Compliance

The table above may seem complicated to the eyes of the traditional lawyer. This is, however, very simple if we learn how to break down the statements in parts. Conditional logical statements: "If (condition, *true, false*)" are often used to choose upon regular activities of our daily life even though we do not often recognize it.

As a way of illustration, consider the fact that we usually go to work during the week and rest during the weekends. In this typical scenario, the conditional formula would be represented as follows: If (it is the weekend, *stay in bed, get up and go to work*). The condition is "If" it is the weekend. If the condition is "true", then you can *stay in bed*. If the condition is "false" (it is not the weekend), then you need *to get up and go to work*.[112]

Conditional logical formulas are also used in various fields for checking one or more conditions on a regular basis. A good example of this is in the accounting sector using the Excel Worksheet program. Accountants often use this method in the Excel sheet to calculate the commissions and bonuses of each employee. This way the Excel conditional formatting function helps to better visualize and calculate relevant data.[113]

In a similar fashion, the way this pseudo code has been designed is to assume that it is legally compliant until one condition is broken and it also works with a conditional "If" formula. In order to make the statements simpler, the legal questions have been substituted for a shorter formula. These are the legal questions (or conditions) that need to be checked in order to be compliant with the new provisions enshrined in the GDPR.

In programming language, the Boolean data type is primarily associated with conditional statements and is denoted as "True" or "False." This can help to understand and check whether certain legal criteria are met or not. If the answer to one question is NO, then it triggers the following statement: "set compliance=false return compliance,"

[112] Weale (2001), p. 6.
[113] Blanc and Vento (2007), p. 192.

which automatically stops the legal analysis and the transaction (e.g., the data transfer) can not be made. However, if the answer to the question is YES, then there is no need to do anything as this is already set as a "True" statement thus legally compliant with the GDPR.

Question 1: *Does your SaaS application deal with sensitive/personal data?* This question refers to sensitive and personal data. This is a very important question that falls directly within the scope of the GDPR. Since the pseudo-code follows a logical order, this question is also related to other questions, especially when it comes to sensitive data such as health or genetic data. In this respect, the GDPR urges data controllers and processors to implement data security measures to prevent unauthorized access and data loss. This involves legal requirements with regard to the encryption and anonymization of personal data and to take the necessary security measures to prevent the loss, disclosure, access or alteration of data.[114] However, such obligations are not enough. They must be implemented into technical standards. Therefore, the following question is more of a technical nature.

Question 2: *Does your SaaS application support native encryption/protection of the data and authentication?* According to Art. 32 (1) (a) of the GDPR, "…the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: pseudonymization and encryption[115] of personal data."[116] This may include different authentication and encryption techniques during data transfer or storage with a range of strength options (i.e., bits used for the encryption) and/or security certification provided and validated by an external third party authority. It is important to note that the Cloud provider does not need to publish the strategy itself, but the ability to comply with this legal and technical requirement.[117]

We often experience this when we use, for example, online banking systems from commercial banks. Most online banking services require their customers to change their passwords on a regular basis. Nevertheless, for security and practical reasons they use other techniques such as automatic passwords generators known as "tokens."[118] Some banks even distribute to their customers some devices that look much like electronic calculators. These devices automatically generate a digit code, which must be used together with the username and password of the client. This method rules out the necessity to choose a password manually every time, saving transaction and deliberation costs. With this new token system, the passcode changes automatically on a regular basis and helps to keep customers' data safe from malicious hackers.[119] This is also a good example of the PbD and Privacy by Default approach[120] set out in the GDPR.

Question 3: *Does your SaaS application give the choice of EU-based data storage location?* This question was designed to cope with the new provisions established in the

---

[114] See, e.g., Barnitzke et al. (2011), pp. 51-55.

[115] For further details with regard to encryption in the scope of the GDPR, see, e.g., Spindler and Schmechel (2016), pp. 163-177.

[116] See Art. 32 (1) (a) of the GDPR; regarding these protective measures see also Recitals 74, 75, 76, 77 and 83 of the GDPR.

[117] Kousiouris, Vafiadis and Corrales (2013), pp. 61-72.

[118] Caelli, Longley and Shain (1989), p. 144.

[119] Williams (2007), p. 12.

[120] Hustinx (2010), pp. 253-255; Chulani et al. (2012), pp. 7-10.

GDPR, which sets out strict rules for the transferring of personal data to third countries outside of the EU. This question is relevant to establish a location constraint mechanism and the ability of the Cloud provider to receive and fulfill requests regarding geographic location of service placement. If the Cloud provider decides to transfer data outside of the EU/EEA Member States, it must ensure that the proper agreements/authorizations are in place prior to the federation.[121] This question is also related to questions 10 and 11 as explained below.

Question 4: *Is your SaaS application dynamically configured for using IaaS/PaaS services?* This question is more of a technical nature, which may have some legal consequences. It refers to the relationship between the software service provider (SaaS) and the infrastructure and platform providers (IaaS and PaaS). It could happen that during the course of the service provisioning the SaaS provider may need to change or move to another Cloud service (IaaS and PaaS). Therefore, the SLA specifications should include a kind of dynamic rating certification scheme as this would imply re-applying the legal conclusion selection.

Question 5: *Are the data or metadata "ownership" rights clearly defined in the contract/SLA?* This question refers to the potential ability of Cloud applications to generate new data out of the data submitted to the Cloud. For example, data mining tools, Artificial Intelligence (AI), data statistics, etc. It is a common practice that some Cloud services do not often specify "ownership" rights of such "derivative" data. Thus, this question would allow end-users to select other Cloud providers in case they prefer a provider with a clear data "ownership" rights policy.

Questions 6 and 7 refer to the problem in which some Cloud providers do not notify consumers when they change their terms and conditions. Cloud providers often reserve the right to change the terms of service unilaterally, at will and at any time. They usually change the terms of services in their website without previous notification to the end-users. This situation was confirmed in the survey carried out in the Cloud Legal Guidelines Report of the OPTIMIS project.[122] These policies need to be re-examined when they change, especially when this is related to customers' data.[123] Therefore, the objective of embedding these legal questions in the smart SLAs is to urge Cloud providers to implement an automated mechanism, which can communicate effectively their customers of any changes in the terms of the SLA.

One humorous anecdotal example refers to the so-called "immortal soul clause," when in 2010 a British on-line videogame retailer (GameStation) temporarily and playfully added a special clause to its terms and conditions.[124] The clause stated that customers granted GameStation the right to claim their "immortal soul." The clause was included in the terms and conditions on the 1st of April (April Fool's Day) as a joke.[125] The result

---

[121] Kousiouris, Vafiadis and Corrales (2013), pp. 61-72.

[122] Forgó, Nwankwo and Pfeiffenbring (2013), p. 20.

[123] See, e.g., Pearson and Charlesworth (2009), p. 137.

[124] House of Commons, Great Britain Parliament, 2014, Responsible Use of data, p. 21, House of Commons, Science and Technology Committee, Fourth Report of Session 2014-15.

[125] The contract read: "By placing an order via this Web site on the first day of the fourth month of the year 2010 Anno Domini, you agree to grant Us a non transferable option to claim, for now and for ever more, your immortal soul. Should we wish to exercise this option, you agree to surrender your immortal soul, and any claim you may have on it, within 5 (five) working days of receiving written notification from gamesation.co.uk or one of its duly authorized minions." See: Fox News Tech, 7,500

was that the overwhelming majority of customers (88%) voluntarily agreed with the terms and conditions of this click-through agreement.[126] This is the equivalent to seventy-five hundred souls "sold" (or "captured") on that single day.[127] This was obviously a joke, however, the company made a serious point: no one reads the fine print, especially if they are suddenly included in the terms and conditions of the contract without previous notification to the users.[128]

Another interesting fact regarding this anecdote, is that the customers were given the choice to tick a box as an opt-out option. That is, the default rule was to automatically grant their "immortal souls" with an option to opt-out. Very few did and the company rewarded them with a £5 voucher. This is in line with the behavioral law and economics claim that "default rules tend to stick" as discussed above in section 4. At the end of April's Fool's Day, the company said that it would not be enforcing "ownership" rights (of their immortal souls), and planned to send an email to their customers revoking such rights.[129]

Question 8: *Do you offer the ability to the user to migrate/extract and reuse their data without any specific and proprietary technology?* This question refers to the data portability and availability issue. The problem is that much emphasis has been laid down in focusing only on strictly technical issues toward increasing interoperability development. There is currently little guidance on how to resolve complex legal issues that arise with regard to data portability.[130] Before developing this criticism in more detail, consider the following hypothetical situation to illustrate this point further: Assume a federated Cloud scenario. In this scenario there is one customer and one service provider both located in the U.K. and an array of infrastructure providers (IPA, IPB, IPC and IPD) located in different jurisdictions. Each of which has its own legislation. Assume further that one of the infrastructure providers, in which end-user's data is stored goes bankrupt. What are the chances of the end-user to recover his or her data if these kinds of circumstances have not been clarified in the contract and the state's legislation of the infrastructure provider in question is debtor friendly?

On a more theoretical level, this could be clarified in the contractual terms i.e., that in cases of bankruptcy the Cloud provider compromises to restore the client's data and agrees to facilitate the means for data migration to another provider. On a more practical level, however, SLAs do not allow much room for negotiation. If the contractual framework provided by the SLA, is also able to clarify data portability issues as a legal concept, as in the bankruptcy example, this will allow the customers to maximize the number of cloud providers. Another example would be the so-called "data hostage" clause, which requires the customer to pay a fee in cases of termination of the contract if the customer wants his or her data to be returned.[131] This sort of clause provides

---

Online Shoppers Unknowingly Sold Their Souls. Available at: http://www.foxnews.com/tech/2010/04/15/online-shoppers-unknowingly-sold-souls.html. Accessed 10 December 2016.

[126] Lori (2012), p. 175.

[127] Lindstrom (2011), p. 225.

[128] Molinaro (2016), p. 35; Goodman (2015), p. 90.

[129] Luzak (2010); Rosenthal (2012).

[130] See, e.g., generally, Zanfir (2012), pp. 149-162.

[131] See, e.g., Carpenter (2010), pp. 1-14.

essentially a risk of data lock-in and customers should be able to recover and migrate their data without further hindrances.

Question 9: *Do you offer the ability to the end-users the right to delete/eliminate their data (so-called "Right to be Forgotten") in the original use service?* This question refers to the deletion or removal of personal data, which is grounded in the provisions enshrined in the previous EU data protection scheme.[132] However, the GDPR explicitly includes the "Right to the Forgotten" as an important legal innovation and not only as codification of the existing law.[133] In this sense, the GDPR refers to this new right as the data subject's right "to obtain from the controller the erasure of personal data concerning him or her without undue delay" and the data controller's obligation "to erase personal data without undue delay" under specific circumstances[134] as laid down in Art. 17. The rationale behind this right is to enable individuals to request the deletion or removal of any kind of personal data[135] where there is no compelling reason for its continued processing. It is therefore not an absolute right and the GDPR provides a list of specific grounds for its removal/deletion. [136]

Questions 10, 11 and 13 refer to the transfer of data to third countries. The use of unmodified Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs) are valuable legal requirements in the framework of the GDPR. Incorporating such options in the SLA framework provides further evidence of an additional safeguard imposed by the law. The pseudo-code it is therefore intended to check a specific instantiation of an SLA (meaning if a specific configuration with given options is legal) or to check if this option is configurable in the SLA. For checking the instantiated SLA, the Cloud provider should add a country/region field and include specific options in the SLA.

In this case, the pseudo-code urges Cloud providers to allow programmatically the inclusion of SCCs and BCRs as a legal text. The BCRs for instance are internal rules (such as a Code of Conduct) adopted by a group of multinational companies who wish to transfer data across different jurisdictions.[137] The automated SLA framework should be able to kick in immediately and stop the processing of data in case the Cloud provider makes a mistake and attempts to make a transfer to a processor or sub-processor that is located outside the group of companies. These checks may include the location of the federated infrastructure provider using a location constraint mechanism. If the target infrastructure provider is inside the jurisdiction of the EU/EEA Member States, then the outsourcing of data may be fulfilled with minimal intervention taking into account the GDPR.[138] If the infrastructure provider is located outside the boundaries of any of the EU/EEA Member States, and, therefore, outside of the scope of the GDPR, then the federation cannot be performed if these checks are not in place in advance.

---

[132] See also *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (es), Mario Costeja González*, number C-131/12.
[133] Lindsay (2014), p. 311.
[134] See Art. 17 of the GDPR; see also Lindsay (2014), p. 311; but see Sobkow (2017), p. 36.
[135] La Fors-Owezynik (2017), p. 129.
[136] See Art. 17 (1) (2) (3) of the GDPR.
[137] Reform of EU Data Protection Rules. EU Commission. Available at: http://ec.europa.eu/justice/data-protection/reform/index_en.htm. Accessed 3 July 2014.
[138] Kousiouris, Vafiadis and Corrales (2013), p. 63.

Question 12: *Do you take measures to prevent data loss (regular backups, replication, etc.)?* Data replication for backup purposes might be seen as one of the main benefits of the Cloud as this prevents data loss in cases of accident. Even from a legal standpoint this might be taken as beneficial if we were to consider data protection and data security issues. However, this also represents a hurdle if we have to consider data location and jurisdictional issues, assuming the customer is not fully aware of where the data has been replicated. In this case the pseudo-code advocates the inclusion of Data Management (DM) specific technical options such as replication rate in the infrastructure. This would allow end-users to track back-up and replication jobs when the databases and Virtual Machines (VMs) grow too fast and may be quickly depleted on the target repository. This will provide greater control for end-users to monitor where their data is located in automated Cloud environments.

Question 15: *Is there any auditing mechanism through which the data subject can be informed (e.g., in case of data breach or data access) about disclosure of their data and when?* This question refers to the data breach notification requirement introduced by the GDPR. According to Art. 33 "in the case of personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority…"[139] Therefore, the pseudo-code attempts to make sure that Cloud providers understand the obligation they have and ensure that they have an effective breach detection and robust auditing mechanism in place.[140]

Finally, the process of checking whether the provider answers are valid can be fully automated if the pseudo-code needed fields (answers to the questions) are captured in a machine understandable format like JavaScript Object Notation (JSON) or eXtensible Markup Language (XML) — or translated to such after exposure of the questions through a relevant user interface — which will enable the automatic inclusion of the needed processing in the general software process. An example of a formal input that would be needed follows for a specific question (question 1):

```
{
        "questionNumber":1,
        "questionText":" Does your SaaS application deal with sensitive/personal data ?"
        "answer":true
}
```

Therefore, if the provider has answered the entire set of 15 questions and has included it in a document (such as a text file) following the previous format, the process can be fully automated. For aiding the process, a software developer can also define a schema, meaning the necessary structure for the overall document that would be needed. The schema for this case appears in Table 3 below. The most important things to observe

[139] See also Articles 33, 34, 83 and Recitals 85, 87 and 88 of the GDPR; Article 29 Working Party, Guidelines on Personal data breach notification under Regulation 2016/679 adopted on 3 October 2017; Müthlein (2017), p. 78.

[140] See, e.g., generally, ENISA Report on "Data breach notifications in the EU." Available at: https://www.enisa.europa.eu/topics/data-protection/personal-data-breaches/personal-data-breach-notification-tool Accessed 30 October 2017.

from this schema is the fact that it dictates those exactly 15 core elements (such as the previously described question 1) need to be included in the document (in order to cover for the entire range of the questions), and each element requires three fields, one with a number value (for the respective question number, with a range from 1 to 15), one text (character string) value for the question text and one Boolean field for indicating the true/false.


```
{
	"type":"object",
	"$schema": "http://legalcompliance.cloud/schema",
	"id": "http://legalcompliance.cloud",
	"required":true,
	"properties":{
		"0": {
			"type":["object","array"],
			"minitems": "15",
			"maxitems": "15",
			"id": "http://legalcompliance.cloud",
			"required":true,
			"properties":{
				"answer": {
					"type":"boolean",
					"id": "http://legalcompliance.cloud/0/answer",
					"required":true
				},
				"questionNo": {
					"type":"number",
					"minimum": "1",
					"maximum": "15",
					"id": "http://legalco...nce.cloud/0/questionNumber",
					"required":true
				},
				"questionText": {
					"type":"string",
					"id": "http://legalcompliance.cloud/0/questionText",
					"required":true
				}
			}
		},

	}
}
```

Table 3 JSON Schema definition for retrieving provider answers

9 Conclusion

The idea of embedding this set of questions into a contractual framework has been inspired by the behavioral approach to law and economics (Nudge Theory). In the opinion of Sunstein and Thaler, *smart disclosure* is one of the most powerful nudging techniques, which can influence a positive behavior or response. Hence, helping individuals to make the "right" choice. These new choices can later be exported through a Graphical User Interface (GUI), for end-users to select which options they need. As a result, this framework will enable a well-designed architecture, which is necessary for developing a consistent and consolidated Smart Contract SLA framework.

Smart contracts are a key component to next-generation blockchain technology. While a typical contract is written using natural language, smart contracts are written in computer code using specific programming languages. Such languages use strict algorithms and can be very complicated for non-programmers (such as lawyers).

Therefore, this article presents the process of creating a *pseudo-code*, which is an intermediate stage between planning and programming. It is essentially a step-by-step outline of the code, which can later be transcribed into any programming language. The whole purpose of a pseudo-code is to make things simpler instead of using real and complex syntax programming language.

The proposed pseudo-code follows a programming logic that allows the implementation of embedding legal concepts into the user interface and related systems. It has been developed in a way to be compliant with the new legal requirements of the GDPR. The design of the pseudo-code includes a set of specific legal and technical questions. These questions are intended to *nudge* Cloud providers and prompt them to disclose relevant information to comply with the new legal requirements set out in the GDPR.

This could be used in the blockchain realm as a piece of code together with the normal blockchain code that validates the right of an entity to access a given asset. For example, even if the owner of the asset (the person owning the data) gives the right to the Cloud provider to access the data, the framework could demand from the provider the answers to the specified pseudo-code questions in order to validate if the specific provider can access the data and therefore protect the user in a seamless manner.

Acknowledgements This work has been partially supported by the EU within the 7th Framework Program under contract ICT-257115 — OPTIMIS (Optimized Infrastructure Services) project. The authors would also like to thank all the researchers involved in the certification model of the ARTIST (Advanced Software-based Service Provisioning and Migration of Legacy Software) project. Without their technical explanations and support, this article would not contain a practical contribution to the state of the art.

References

Agarwal B, Tayal M, Gupta S (2010) Software Engineering and Testing. Jones and Bartlett Publishers, Sudbury MA

Anderson D (2015) A Question of Trust. Williams Lea Group, London

Asharaf S, Adarsh S (2107) Decentralized Computing Using Blockchain Technologies and Smart Contracts: Emerging Research and Opportunities. IGI Global, Hershey PA

Balasubramanyam S (2013) Cloud-Based Development Using Classic Life Cycle Model. In: Mahmood Z, Saeed S (eds) Software Engineering Frameworks for the Cloud Computing Paradigm. Springer, London

Bar-Gill O (2012) Seduction by Contract: Law, Economics, and Psychology in Consumer Markets. Oxford University Press, Oxford

Barlow RJ, Barnett AR (1998) Computing for Scientists: Principles of Programming with Fortran 90 and C++. John Wiley & Sons, Chichester

Barnitzke B et al (2011) Legal restraints and security requirements on personal data and their technical implementation in clouds, Workshop for E-contracting for clouds. eChallenges. Available at: http://users.ntua.gr/gkousiou/publications/eChallenges2011.pdf. Accessed 1 Sept 2016

Ben-Porath S (2010) Tough Choices: Structural Paternalism and the Landscape of Choice. Princeton University Press, Princeton

Bernheim R et al. (2015) Essentials of Public Health Ethics. Jones and Bartlett Learning, Burlington MA

Blanc I, Vento C (2007) Performing with Microsoft Office 2007: Introductory. Cengage Learning, Boston

Bragg S (2006) Outsourcing: A Guide to Selecting the Correct Business Unit, Negotiating the Contract, Maintaining Control of the Process, 2nd edn. John Wiley & Sons, Hoboken

Briggs P, Jeske D, Coventry L () Behavior Change Interventions for Cybersecurity. In: Little L, Sillence E, Joinson A (eds) Behavior Change Research and Theory: Psychological and Technological Perspectives. Academic Press, Amsterdam

Brooks D (1997) Problem Solving with Fortram 90: For Scientists and Engineers. Springer, New York

Busch C (2016) The Future of Pre-Contractual Information Duties: From Behavioral Insights to Big Data. In: Twigg-Flesner C (ed) Research Handbook on EU Consumer and Contract Law, Edward Elgar Publishing, Cheltenham

Caelli W, Longley D, Shain M (1989) Information Security for Managers. Stockton Press, New York

Cahn N (2013) The New Kinship: Constructing Donor-Conceived Families. New York University Press, New York

Carnevale C (2017) Future of the CIO: Towards an Enterpreneurial Role. In: Bongiorno G, Rizzo D, Vaia G (eds) CIOs and the Digital Transformation: A New Leadership Role. Springer, Cham

Carpenter R (2010) Walking from Cloud to Cloud: The Portability Issue in Cloud Computing. Washington Journal of Law, Technology & Arts 6(1):1-14

Carstensen J, Morgenthal J, Golden B (2012) Cloud Computing: Assessing the Risks. IT Governance Publishing, Cambridgeshire

Cavoukian A (2015) Evolving FIPPs: Proactive Approaches to Privacy, Not Privacy Paternalism. In: Gutwirth S, Leenes R, de Hert P (eds) Reforming European Data Protection Law. Springer, Dordrecht

Chulani I et al. (2012) Technical Implementation of Legal Requirements, Exploitation of the Toolkit in Use Cases and Component Licenses, p. 23, Cloud Legal Guidelines, OPTIMIS Deliverable 7.2.1.3. Available at: http://www.optimis-project.eu/sites/default/files/content-files/document/d7213-cloud-legal-guidelines.pdf. Accessed 10 Oct 2017

Corrales M, Jurcys P (2016) Cass Sunstein, Why Nudge: The Politics of Libertarian Paternalism, New Haven/London: Yale University Press, 2014, 208 pp, pb, £10.99. The Modern Law Review 79(3):533-536

Cross R, O'Neil I, Dixey R (2013) In: Dixey R, Health Promotion: Global Principles and Practice. CAB International, Oxfordshire

Cwalina W, Falkwoski A, Newman B (2015) Persuasion in the Political Context: Opportunities and Threats. In: Stewart D (ed) The Handbook of Persuasion and Social Marketing, Vol. 1: Historical and Social Foundations. Praeger, Santa Barbara CA

D'Aquisto et al. (2015) Privacy by Design in Big Data: An Overview of Privacy Enhancing Technologies in the Era of Big Data Analytics. European Union Agency for Network and Information Security (ENISA).

Debbabi M et al. (2010) Verification and Validation in Systems Engineering: Assessing UML/SysML Design Models. Springer, Berlin

Detels R, Gulliford M (2015) Oxford Textbook of Global Public Health, 6th (edn), Vol. 1. Oxford University Press, Oxford

Diamond P, Vartiainen H (2007) Behavioral Economics and Its Applications. Princeton University Press, Princeton

Ford W (2015) Numerical Linear Algebra with Applications: Using MARLAB. Elsevier, Amsterdam

Forgó N, Nwankwo I, Pfeiffenbring J (2013) Cloud Legal Guidelines Final Report, Deliverable 7.2.1.4. OPTIMIS European funded project

Fosch Villaronga (2018) Legal Frame of Non-social Personal Care Robots. In: Husty M, Hofbaur M (eds) New Trends in Medical and Service Robots: Design, Analysis and Control. Springer, Cham

Fung A, Graham M, Weil D (2007) Full Disclosure: The Perils and Promise of Transparency. Cambridge University Press, Cambridge

Galis A (2000) Multi-Domain Communication Management Systems. CRC Press, Boca Ratón

Gjermundrød H, Dionysiou I, Costa K (2016) privacyTracker: A Privacy-by-Design GDPR-Compliant Framework with Verifiable Data Traceability Controls. In: Casteleyn S, Dolog P, Pautasso C (eds) Current Trends in Web Engineering. ICWE 2016 International Workshops DUI, TELERISE, SoWeMine, and Liquid Web, Lugano Switzerland, June 6-9, 2016, Revised Selected Papers. Springer, Cham

Goodman M (2015) Future Crimes: Inside The Digital Underground and the Battle For Our Connected World. Transworld Publishers (Bantam Press), London

Gries D, Gries P (2005) Multimedia Introduction to Programming Using Java. Springer, New York

Griggs S (2013) 5 Hidden Problems with Cloud SLAs http://www.thewhir.com/blog/5-hidden-problems-cloud-slas Accessed 10 May 2017
Grynbaum M, Taylor K (2012) Bloomberg Defends Grading System Derided by Restaurateurs, The New York Times http://www.nytimes.com/2012/03/07/nyregion/restaurant-grading-system-under-fire-gets-mayors-backing.html. Accessed 10 May 2017
Hamilton D, Zufiaurre B (2014) Blackboards and Bootstraps: Revisioning Education and Schooling. Sense Publishers, Rotterdam
Hennicker R, Koch N (2001) Modeling the User Interface of Web applications with UML. In: Evans A et al. (eds) Practical UML-Based Rigorous Development Methods – Countering or Integrating the eXtremists, Workshop of the pUML-Group held together with UML 2001, Toronto, Canada. GI, Gesselschaft für Informatik, Bonn
Heshmat S (2015) Addiction: A Behavioral Economic Perspective. Routledge, New York
Hijmans H (2016) The European Union as Guardian of Internet Privacy: The Story of Art. 16 TFEU. Springer, Cham
Ho D (2012) Fudging the Nudge: Information Disclosure and Restaurant Grading. The Yale Law Journal 122(3):574-688
Hogan J (2017) Lawyers Learning to Code? To do or not to do, that is the question! https://www.cli.collaw.com/latest-on-legal-innovation/2017/08/16/should-lawyers-learn-to-code Accessed 10 Oct 2017
Horrigan J (2008) Use of Cloud Computing Applications and Services http://www.pewinternet.org/2008/09/12/use-of-cloud-computing-applications-and-services/ Accessed 10 Oct 2017
Hossain S (2013) Cloud Computing Terms, Definitions and Taxonomy. In: Bento A, Aggarwal A (eds) Cloud Computing Service and Deployment Models: Layers and Management. Business Science Reference (IGI Global), Hershey PA
Howard A (2012) What is smart disclosure? “Choice engines” are helping consumers make smarter decisions through personal and government data http://radar.oreilly.com/2012/04/what-is-smart-disclosure.html. Accessed 10 May 2017
Hustinx P (2010) Privacy by Design: Delivering the Promises. Identity in the Information Society 3(2):253-255
ISRD Group (2007) Structured System Analysis and Design. Tata McGraw-Hill Publishing, New Delhi
ITL Education Solutions (2006) Introduction to Information Technology. Dorling Kindersley, New Delhi
John P et al. (2013) Nudge, Nudge, Think, Think: Experimenting with Ways to Change Civic Behavior. Bloomsbury, London
Jolls C (2010) Behavioral Economics and the Law. Foundations and Trends in Microeconomics 6(3):176-263
Kamthane A, Kamal R (2012) Computer Programming and IT. ITL Education Solutions Ltd., New Delhi
Kimball G (2010) Outsourcing Agreements: A Practical Guide. Oxford University Press, Oxford

King A, Squillante M (2005) Service Level Agreements for Web Hosting Systems. In: Labbi A (ed) Handbook of Integrated Risk Management for E-Business: Measuring, Modeling, and Managing Risk. J. Ross Publishing, Boca Ratón

Kost de Sevres N (2016) The Blockchain Revolution, Smart Contracts and Financial Transactions. Available at: https://www.dlapiper.com/en/uk/insights/publications/2016/04/the-blockchain-revolution/. Accessed 10 Oct 2017

Kousiouris G, Vafiadis G, Corrales M (2013) A cloud provider description schema for meeting legal requirements in cloud federation scenarios. In: Douligeris et al (eds) Collaborative, trusted and privacy-aware e/m-services, 12th IFIP WG 6.11 conference on e-business, e-services, and e-society, I3E 2013, Athens, Greece, Proceedings. Springer, Heidelberg

La Fors-Owezynik K (2017) Profiling 'Anomalies' and the Anomalies of Profiling: Digitilized Risk Assessments of Dutch Youth and the New European Data Protection Regime. In: Adams S, Purtova N, Leenes N (eds) Under Observation: The Interplay Between eHealth and Surveillance. Springer, Cham

Leitzel J (2015) Concepts in Law and Economics: A Guide for the Curious. Oxford University Press, Oxford

Lessig (2001) The Future of Ideas, 1st edn. Random House, New York

Lessig L (2006) Code. Version 2.0. Basic Books, New York

Lindahl T, Stikvoort B (2015) Nudging – The New Black in Environmental Policy? Tryckt hos ScandBooks, Falun

Lindsay D (2014) The Right to be Forgotten in European Data Protection Law. In: Witzleb N, Lindsay D, Paterson M (eds) Emerging Challenges in Privacy Law. Cambridge University Press, Cambridge

Lindstrom M (2011) Brandwashed: Tricks Companies Use to Manipulate Our Minds and Persuade Us to Buy, 1st edn. Crown Business, New York

Lori A (2012) I Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy. Free Press, New York

Luzak J (2010) One Click Could Save Your Soul, Recent Developments in European Consumer Law. Available at: http://recent-ecl.blogspot.jp/2010/05/one-click-could-save-your-soul.html. Accessed 10 Dec 2016

Lynskey O (2015) The Foundations of EU Data Protection Law. Oxford University Press, Oxford

Marc et al (2015) Indexing Publicly Available Health Data with Medical Subject Headings (MeSH): An Evaluation of Term Coverage. In: Sarkar I, Georgiou A, Mazzoncini de Azevedo Marques, P, (2015), MEDINFO 2015: eHealth-enabled Health, Proceedings of the 15th World Congress on Health and Biomedical Informatics. IOS Press, Amsterdam

Mc Nealy J, Flowers A (2015) Privacy Law and Regulation: Technologies, Implications and Solutions. In: Zeadally S, Badra M (eds) Privacy in a Digital, Networked World: Technologies, Implications and Solutions. Springer, Cham

Millham R (2012) Software Asset Re-Use: Migration of Data-Intense Legacy System to the Cloud Computing Paradigm. In: Yang H, Liu X (eds) Software Reuse in the

Emerging Cloud Computing Era. Information Science Reference (IGI Global), Hershey
Molinaro V (2016) The Leadership Contract: The Fine Print to Becoming an Accountable Leader. John Wiley & Sons, Hoboken
Morabito V (2017) Business Innovation Through Blockchain: The B3 Perspective. Springer, Cham
Moskowitz S (2017) Cybercrime and Business: Strategies for Global Corporate Security. Elsevier, Oxford
Muresan G (2009) An Integrated Approach to Interaction Design and Log Analysis. In: Jansen B, Spink A, Taksa I (eds) Handbook of Research on Web Log Analysis. Information Science Reference (IGI Global), Hershey
Müthlein T (ed) (2017) Datenschutz-Grundverordnung – General Data Protection Regulation. Datakontext, Frechen
Myler H (1998) Fundamentals of Engineering Programming with C and Fortram. Cambridge University Press, Cambridge
Naughton J, Dredge S (2011) Cloud Computing: The Lowdown. Available at: https://www.theguardian.com/technology/2011/nov/06/cloud-computing-guide-history-naughton. Accessed 10 Oct 2017
Olislaegers (2012) Early Lessons Learned in the ENDORSE Project: Legal Challenges and Possibilities in Developing Data Protection Compliance Software. In: Camenish J et al. (eds) Privacy and Identity Management for Life. Springer, Heidelberg
Oveergaard G (1999), A Formal Approach to Collaborations in the Unified Modeling Language. In: France R, Rumpe B (eds) UML'99 – The Unified Modeling Language: Beyond the Standard, Second International Conference For Collins, CO, USA, October 28-30, Proceedings. Springer, Berlin
Patel N (2005) Critical Systems Analysis and Design: A Personal Framework Approach. Routledge, New York
Pearson S, Charlesworth A (2009) Accountability as a Way Forward for Privacy Protection in the Cloud. In: Jaatun M, Zhao G and Rong C (eds) Cloud Computing, 1st. International Conference, CloudCom 2009, Beijing, China, December 2009, Proceedings. Springer, Berlin
Post D (2009) In Search of Jefferson's Moose: Notes on the State of Cyberspace. Oxford University Press, Oxford
Quelle C (2016) Not Just User Control in the General Data Protection Regulation: On the Problems with Choice and Paternalism, and on the Point of Data Protection. In: Lehmann A et al. (eds) Privacy and Identity Management: Facing up to Next Steps. Springer, Cham
Quigley M, Stokes E (2015) Nudging and Evidence-Based Policy in Europe: Problems of Normative Legitimacy and Effectiveness. In: Alemanno A, Sibony A-L (eds) Nudge and the Law: A European Perspective, Modern Studies in European Law. Hart Publishing, Oxford
Roberto C, Kawachi I (2016) (eds) Behavioral Economics and Public Health. Oxford University Press, Oxford
Rosenthal E (2012) I Disclose…Nothing. The New York Times. Available at: http://www.nytimes.com/2012/01/22/sunday-review/hard-truths-about-disclosure.html?_r=0. Accessed 10 Dec 2016

Schweizer M (2016) Nudging and the Principle of Proportionality. In: Mathis K, Thor A (eds) Nudging – Possibilities, Limitations and Applications in European Law and Economics. Springer, Cham
Simpson T (2014) Computing and the Search for Trust. In: Richard Harper (ed) Trust, Computing, and Society. Cambridge University Press, Cambridge
Sheshasaayee A, Swetha T (2016) SLA Based Utility Analysis for Improving QoS in Cloud Computing. In: Chandra S et al. (eds) Information Systems Design and Intelligent Applications, Proceedings of the 3rd International Conference, India 2016, Vol. 3. Springer, New Delhi
Sobkow B (2016) Forget Me, Forget Me Not – Redefining the Boundaries of the Right to be Forgotten to Address Current Problems and Areas of Criticism. In: Schweichhofer E et al. (eds) Privacy Technologies and Policy, 5th Annual Privacy Forum, APF 2017, Vienna, Austria, June 7-8, 2017, Revised Selected Papers. Springer, Cham
Spindler G, Schmechel P (2016) Personal Data and Encryption in the European General Data Protection Regulation. JIPITEC 7:163-177
Sunstein C (2014a) Simpler: The Future of Government. New York: Simon & Schuster
Sunstein C (2014b) Why Nudge? The Politics of Libertarian Paternalism, Storrs Lectures on Jurisprudence. Yale University Press, New Haven
Sunstein C (2015a) Nudging and Choice Architecture: Ethical Considerations. Discussion Paper No. 809. Yale Journal on Regulation (Forthcoming)
Sunstein C (2015b) Choosing Not To Choose: Understanding the Value of Choice. Oxford University Press, Oxford
Svantesson D (2013) Extraterritoriality in Data Privacy Law. Ex Tuto Publishing, Copenhagen
Svirskas B (2004) Dynamic Management of Business Service Quality in Collaborative Commerce Systems. In: Mendes M, Suomi R, Passos C (eds) Digital Communities in a Networked Society: e-Commerce, e-Business and e-Government. Kluwer Academic Publishers, New York
Swan M (2015) Blockchain: Blueprint for a New Economy, 1st edn. O'Reilly, Sebastopol CA
Tereszkiewicz P (2016) Neutral Third-Party Counselling as Nudge Toward Safer Financial Products? In: Mathis K, Tor A (eds) Nudging – Possibilities, Limitations and Applications in European Law and Economics. Springer, Cham
Thaler R (2009) Opting In vs. Opting Out, The New York Times. Available at: http://www.nytimes.com/2009/09/27/business/economy/27view.html?_r=0. Accessed 20 Dec 2016
Thaler R, Sunstein C (2009) Nudge: Improving Decisions about Health, Wealth, and Happiness. Penguin Books Ltd., London
Thouvenin F (2017) Big Data of Complex Networks and Data Protection Law: An Introduction to an Area of Mutual Conflict. In: Dehmer M et al. (eds) Big Data of Complex Networks. CRC Press, Boca Ratón
Van Alsenoy B et al. (2015) From Social Media Service to Advertising Network: Analysis of Facebook's Revised Policies and Terms, Report, Draft Version 1.2
Varshney A (2017) Types of Blockchain – Public, Private and Permissioned. Available at: https://blog.darwinlabs.io/types-of-blockchain-public-private-and-permissioned-5b14fbfe38d4. Accessed 10 Jan 2018

Voigt P, von dem Bussche A (2017) The EU General Data Protection Regulation (GDPR): A Practical Guide. Springer, Cham
Wattenhofer R (2016) The Science of the Blockchain. Inverted Forest Publishing, s. l.
Weale D (2001) The Smart Guide to Excel 2000 Further Skills: A Progressive Course for More Experienced Users. Continuum, London.
Whyte K et al. (2015) Nudge, Nudge or Shove, Shove – The Right Way for Nudges to Increase the Supply of Donated Cadaver Organs. In: Caplan A, Mc Cartney J, Reid D (eds) Replacement Parts: The Ethics of Procuring and Replacing Organs in Humans. Georgetown University Press, Washington, DC
Williams G (2007) Online Business Security Systems. Springer, New York
Willis O (2015) *Behavioral Economics for Better Decisions*, ABC.net Available at: http://www.abc.net.au/radionational/programs/allinthemind/better-life-decisions-with-behavioural-economics/6798918 Thaler Accessed 25 June 2015
Wisman T (2017) Privay, Data Protection and E-Commerce. In: Lodder A, Murray A (eds) EU Regulation of E-Commerce. Edward Elgar Publishing, Cheltenham
Zamir E, Teichman D (2014) (eds) The Oxford Handbook of Behavioral Economics and the Law. Oxford University Press, Oxford
Zanfir G (2012) The Right to Data Portability in the Context of the EU Data Protection Reform. International Data Privacy Law 2(3):149-162