Examining How GDPR Challenges Emerging Technologies

Author(s): Rania El-Gazzar and Karen Stendal

Source: *Journal of Information Policy*, 2020, Vol. 10 (2020), pp. 237-275

Published by: Penn State University Press

Stable URL: https://www.jstor.org/stable/10.5325/jinfopoli.10.2020.0237

EXAMINING HOW GDPR CHALLENGES EMERGING TECHNOLOGIES

Rania El-Gazzar and Karen Stendal

ABSTRACT

Emerging technologies, particularly cloud computing, blockchain, Internet of Things, and artificial intelligence, have received noticeable attention from research and industry. These technologies contribute to innovation in public and private organizations, but threaten the privacy of individuals. The natural characteristics of these technologies are challenged by the new general data protection regulation (GDPR). In this article, we examine the compliance challenges between these technologies' characteristics and GDPR both individually and when combined. We identified compliance opportunities related to the characteristics of these technologies. We discuss possible approaches to address the compliance challenges identified and raise questions for further research in the area.

Keywords: GDPR, cloud computing, blockchain, Internet of Things, artificial intelligence

There has long been a consensus among researchers that technological developments are growing at a speed that legal frameworks cannot catch.[1] Emerging technologies, such as cloud computing (CC), blockchain (BC), Internet of Things (IoT), and artificial intelligence (AI), share a common characteristic: an openness that makes them remarkably innovative.[2] This openness is perceived by organizations and societies as an enabler for innovation in our interconnected world. Each emerging technology also offers appealing benefits. CC offers access to scalable distributed Information Technology (IT) resources and skills and reduces capital expenditures.[3] BC offers security and transparency,

1. Kshetri; Herian; Burri and Schär.
2. Avital et al.; Loebbecke et al.; Stankovic; De Magalhães Santos.
3. Venters and Whitley.

Rania El-Gazzar: University of South-Eastern Norway
Karen Stendal: University of South-Eastern Norway
DOI: 10.5325/jinfopoli.10.2020.0237

such as immutability and traceability of transactions.[4] IoT enables the generation of real-time rich data from IoT devices, increasing productivity and improving quality of life.[5] AI offers autonomous machine learning (ML), prediction, and problem-solving techniques to enable effective improvements in various production and service industries.[6]

According to Gartner's hype cycle, CC has become the ideal ubiquitous infrastructure technology for BC, IoT, and AI.[7] Moreover, all four emerging technologies are here to stay with possibilities for further experimentation.[8] However, the legal challenges concerning CC, BC, IoT, and AI are enormous, especially once the new General Data Protection Regulation (GDPR) came into effect in May 2018. The purpose of GDPR was to relate existing legislation to current technological trends and assure compliance across the European Union (EU).[9] GDPR applies to all organizations offering products and services to EU citizens regardless of whether they are based inside or outside the EU.[10] GDPR also applies to all organizations processing the personal data of data subjects residing in the EU regardless of where they are offering products or services to them and whether the processing of their personal data is manual or automated.[11] In additions, GDPR applies to the development lifecycle of technological solutions under Article 25, data protection by design and by default.[12] The increasing tendency of organizations to adopt emerging technologies has challenged both the adopting organizations and the providers of those technologies in terms of their compliance with GDPR.[13] These technologies may also present challenges for lawmakers in terms of accommodating societal demands for innovation.

Adopters and providers of CC, BC, IoT, and AI solutions are starting to understand the GDPR principles in order to apply the necessary technical and organizational measures to become GDPR-compliant; however, these

4. Avital et al.
5. Makhdoom et al.
6. Sousa et al.; Achmat and Brown.
7. Panetta, "5 Trends Appear on the Gartner Hype."
8. Panetta, "5 Trends Emerge in the Gartner Hype."; Panetta, "5 Trends Appear on the Gartner Hype."
9. Gobeo et al.
10. Article 3, GDPR.
11. Article 3, Recital 15, GDPR.
12. Tamburri.
13. Miri et al.; Duncan and Zhao.

measures are daunting.[14] Thus, to understand the implications of GDPR, the characteristics of CC, BC, IoT, and AI deserves a critical review.

GDPR restricts the use of CC services offered by non-EU cloud providers, including personal data storage locations and the power of third parties or governments to access the data without consent from data subjects who are in the EU.[15] GDPR also challenges the immutable nature of BC with Article 17, the right to be forgotten, because BC data cannot be altered or deleted.[16] Hence, we were motivated to synthesize the GDRP compliance challenges faced by emerging technologies, particularly CC, BC, IoT, and AI, and their implications for adopters and providers. As such, we developed the following research question: *How does GDPR challenge the nature of emerging technologies?*

The section Background on GDPR and its Predecessor provides a brief historical background of GDPR, including its principles and data subject rights. The section Emerging Technologies and GDPR provides background information on each technology, including fundamental definitions and characteristics, along with an overview of the issues and conflicts between the four emerging technologies and GDPR. The section Discussion and Conclusion brings in key discussion points and concludes the article.

Background on GDPR and its Predecessor

In 1995, the European Union Directive 95/46/EC was enacted to protect the processing and free movement of individuals' personal data.[17] Each EU member state drew up its own local law from Directive 95/46/EC, which fragmented the implementation of data protection across the EU, resulting in different levels of protection of the processing of personal data, which prevented the free flow of personal data throughout the EU.[18] Those differences had an undesirable impact on economic activities across the EU, made the compliance process tedious, and slowed down the authorities in executing their responsibilities under EU law.[19] Thus, Directive 95/46/EC

14. Tamburri.
15. Burri and Schär.
16. Herian.
17. EUR-Lex.
18. Ibid.
19. Ibid.

resulted in inconsistent legislation among the EU member states, which posed significant risks to the protection of individuals who are in the EU (i.e., data subjects), especially in online activities.[20] The different levels of protection of the rights of data subjects during the processing of personal data prevented the free flow of personal data throughout the EU.[21] More importantly, Directive 95/46/EC made it difficult to implement privacy laws in foreign jurisdictions.[22] In addition, the narrow territorial scope of Directive 95/46/EC made the EU market less accessible by organizations established outside the EU, especially given the rapid adoption of digital platforms that move data across borders.[23]

Furthermore, events, such as Google Spain (*Google Spain v AEPD and Mario Costeja González*), have served as an eye opener regarding the need for stronger protection of data subject rights. Especially, the right to be forgotten when disclosed data about the data subject are no longer relevant.[24] This manifested in a battle between Mario Costeja González and Google in 2009, when Google search engine displayed a link to a newspaper article published in 1998. The article revealed that Mr. González's home was subject to a real-estate auction to pay off his debts, which had been resolved.[25] As the matter became irrelevant to Mr. González and the public interest, in 2014, the Court of Justice of the European Union (CJEU) ruled that search engine operators are obliged to remove links to web pages from their result list if requested by the data subject.[26]

Thus, the EU Commission offered suggestions for a new regulation for general data protection, and GDPR was agreed upon by the EU parliament in 2016 and came into effect on May 25, 2018.[27] GDPR contains 99 formal articles that stipulate the obligatory requirements for data controllers and data processors, along with 173 recitals that provide insights into the context of those articles. Unlike a directive, which is a legislative act that sets out a goal that all EU countries must achieve through their own independently created laws, GDPR is a regulation, which means that it is

20. Ibid.
21. Repealing Directive 95/46/EC (9): https://eur-lex.europa.eu/eli/reg/2016/679/oj.
22. Burri and Schär.
23. Ibid.
24. Ibid.
25. Ibid.
26. Ibid.
27. EUR-Lex.

a binding legislative act that must be applied in its entirety across the EU.[28] Administrative fines for violating this regulation vary depending on the severity of those violations.[29]

GDPR addresses the drawbacks inherent in Directive 95/46/EC; it cuts out the administrative hassle of handling several fragmented data protection laws.[30] GDPR allows for the free flow of data across EU member states and facilitates the increased cross-border processing of personal data due to rapid technological developments, while ensuring a high level of protection of personal data.[31] GDPR also changed the responsibilities of controllers and processors, as well as set the extraterritorial applicability scope.[32] The extraterritorial scope of GDPR applies to the processing of personal data: (1) establishments of controller or processor in the EU regardless of whether the processing takes place within the EU or not; (2) establishments of controller or processor outside the EU that offer goods and services to data subjects in the EU and monitor their behavior that takes place in the EU. However, the French Data Protection Supervisory Authority (CNIL) has revived battle of the right to be forgotten between Google Spain and Mr. González from 2015, regarding the territorial scope of applicability of delisting.[33] CNIL argued that Google must delist links universally, while the CJEU ruled that Google is not obliged to apply the European right to be forgotten globally, which limits the territorial scope of that right within the borders of the 28 Member States.

Personal data categories were added under GDPR, such as location data and online identifiers.[34] Online identifiers are identifiers provided by natural persons' devices, applications, tools, and protocols, such as Internet protocol (IP) addresses, cookie identifiers, or other identifiers, such as radio frequency identification (RFID) tags.[35] When combined with unique identifiers, online identifiers can be used to create profiles of the natural persons and identify them.

---

28. Regulations, Directives and other acts: https://europa.eu/european-union/eu-law/legal-acts_en.

29. Article 83 (4-5), GDPR.

30. Repealing Directive 95/46/EC (8): https://eur-lex.europa.eu/eli/reg/2016/679/oj.

31. Burri and Schär; EUR-Lex.

32. Burri and Schär.

33. Google v CNIL Case C-507/17: The Territorial Scope of the Right to be Forgotten Under EU Law: https://europeanlawblog.eu/2019/10/29/google-v-cnil-case-c-507-17-the-territorial-scope-of-the-right-to-be-forgotten-under-eu-law/.

34. Article 4 (1), GDPR.

35. Article 4 (1), Recital 30, GDPR.

The processing of personal data carries the same meaning under Directive 95/46/EC and GDPR. It is defined under GDPR as follows:

> any operation or set of operations which is performed on personal data or on sets of personal data, whether by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.[36]

Under GDPR, pseudonymization risks the reidentification of data subjects and is described as follows:

> the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.[37]

Even though the definitions of the controller and the processor are the same in Directive 95/46/EC and GDPR, their responsibilities changed under GDPR.[38,39] The controller is defined as follows:

> the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.[40]

The processor is defined as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."[41]

---

36. Article 4 (2), GDPR.
37. Article 4 (5), GDPR.
38. Article 2, Directive 95/46/EC.
39. Article 4, GDPR.
40. Article 4 (7), GDPR.
41. Article 4 (8), GDPR.

The controller is responsible for implementing appropriate technical and organizational measures to ensure and demonstrate that processing is compliant with GDPR; the controller shall implement data protection policies and adhere to approved codes of conduct to demonstrate its compliance.[42] The controller is required to use only processors who provide sufficient guarantees to implement appropriate technical and organizational measures so that the processing complies with GDPR and ensures the protection of the rights of the data subject.[43] Under GDPR, the processor may adhere to approved codes of conduct to demonstrate that sufficient guarantees are provided.[44] The processor shall not engage other processors without receiving prior specific or general written authorization from the controller and shall inform the controller of any intended changes concerning the addition or replacement of other processors so that the controller has the opportunity to object to such changes.[45]

Furthermore, the processing of personal data by the processor shall be governed by a contract based on documented instructions from the controller; the contract shall set the duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, and the obligations and rights of the controller.[46] If a processor engages another processor to carry out specific processing activities on behalf of the controller, the same data protection obligations in the contract between the controller and the initial processor shall be imposed on the new processor; additionally, the initial processor shall remain fully liable to the controller for the performance of that other processor.[47]

Under GDPR, personal data breach is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of or access to personal data transmitted, stored, or otherwise processed.[48] GDPR requires the controller to notify the supervisory authority of a personal data breach without undue delay and no later than 72 hours after he or she becomes aware of it, where feasible.[49] At a minimum, the notification must contain the following: (1) the nature of the

42. Article 24 (1), (2), and (3), GDPR.
43. Article 28 (2), GDPR.
44. Article 28 (5), GDPR.
45. Article 28 (2), GDPR.
46. Article 28 (3), GDPR.
47. Article 28 (4), GDPR.
48. Article 4 (12), GDPR.
49. Article 33 (1), GDPR.

data breach, including the categories and number of data subjects affected and the categories and number of personal data records affected; (2) the name and contact details of a contact point from whom more information can be obtained; (3) the likely consequences of the personal data breach; and (4) the measures taken or proposed by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.[50]

Furthermore, GDPR set the scope of extraterritorial applicability to include controllers and processors that are not established in the EU when their processing activities are related to offering goods or services to and/or monitoring the behavior of EU data subjects.[51]

GDPR Principles

GDPR builds on the following seven key principles to which organizations processing personal data about EU citizens must adhere[52]:

1. *Lawfulness, fairness, transparency:* Personal data shall be processed lawfully, fairly, and in a transparent manner in relation to the data subject.
2. *Purpose limitation:* Personal data shall be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes shall not be considered to be incompatible with the initial purposes.
3. *Data minimization:* Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
4. *Accuracy:* where personal data shall be accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
5. *Storage limitation:* Personal data shall be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed

50. Article 33 (3), GDPR.
51. Article 3 (2), (2), and (3), GDPR.
52. Article 5, GDPR.

solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to implementation of the appropriate technical and organizational measures required by GDPR in order to safeguard the rights and freedoms of the data subject.

6. *Integrity and confidentiality:* Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.
7. *Accountability:* The controller shall be responsible for, and be able to demonstrate compliance with the above six principles.

Data Subject Rights

The data subjects are granted a set of stronger rights under GDPR than Directive 95/46/EC regarding the processing of their personal data.[53] Transparency and modality are important for data subjects to exercise their rights; the controller shall provide the data subjects with any information related to the processing of their personal data and actions taken without delay on the request of the data subject for exercising his or her rights free of charge, unless the request of the data subject is unfounded or excessive.[54] This information shall be provided by electronic means in a clear and concise written form.

Regardless of whether the personal data collected directly or indirectly, the controller shall inform the data subjects of their rights under GDPR, the purpose of processing their personal data, the period of storing the data, the intentions to further process their personal data for other purposes, as well as the existence of automated decision-making, including profiling and meaningful information about the logic involved.[55] The controller shall inform the data subjects about their right to request from the controller access,[56] rectification,[57] and erasure of personal data.[58] Additionally, the controller shall inform the data subjects of their right to object to

53. Burri and Schär.
54. Article 12, GDPR.
55. Article 13 and Article 14, GDPR.
56. Article 15, GDPR.
57. Article 16, GDPR.
58. Article 17, GDPR.

processing their personal data,[59] restriction of processing,[60] data portability (i.e., receive their personal data in a structured and machine-readable format),[61] and withdraw consent at any time without affecting the lawfulness of processing based on consent before its withdrawal.[62] The controller shall also inform the data subjects about the existence of automated decision-making, including profiling and any meaningful information about the logic involved[63] so that the data subjects can exercise their right not to be subject to automated decision-making and profiling that affects them significantly.[64] Providing the above information to the data subjects enables them to freely give, specific, informed, and unambiguous consent by a statement or a clear affirmative action to the processing of their personal data.[65]

In this section, we provided an overview of GDPR and its predecessor legal framework. We presented the key principles and data subject rights under GDPR, which guide our legal analysis in the next section.

Emerging Technologies and GDPR

In this section, we explore four emerging technologies (i.e., CC, BC, IoT, and AI) as enablers for innovation in societies and organizations.[66] Although these emerging technologies offer a variety of compelling solutions and benefits, they also pose major technical complexities and legal challenges. The technical complexities stem from their individual nature and from combining them into a single solution.[67] There is a never-ending debate whether CC, BC, IoT, and AI comply with GDPR or not. GDPR requires that the processing of personal data by organizations is lawful, fair, and transparent. The key characteristics in each technology may lead to compliance with or violation of GDPR principles and data subject rights.[68] In the following subsections, we provide an overview of the definitions

59. Article 21, GDPR.
60. Article 18, GDPR.
61. Article 20, GDPR.
62. Article 7, GDPR.
63. Article 13 (2)f and Article 14 (2)g, GDPR.
64. Article 22 (1), GDPR.
65. Article 4 (11), GDPR.
66. Xu et al.; Perera et al.
67. Dorri et al.; Samaniego and Deters; Reyna et al.
68. Herian; Truong et al.; Duncan and Whittington; Pham.

and characteristics of CC, BC, IoT, and AI and discuss GDPR compliance issues related to each technology.

CC and GDPR

The National Institute of Standards and Technology (NIST) defined CC as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".[69] The main three CC service models are Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).[70] In all three cloud service models, the customers do not manage or control the cloud infrastructure but have limited configuration settings to control.[71] NIST's definition of CC conveys the technical characteristics of CC, including that the computing resources are on-demand self-service resources, accessed over the network, pooled and shared among customers, and rapidly scaled as needed; in addition, their usage is automatically monitored.[72] Next, we will analyze CC characteristics that raise GDPR compliance issues, which are summarized in Table 1.

Virtualization is a fundamental characteristic of the shared pool of computing resources in a cloud environment.[73] This shared pool is a double-edged sword; it defines the innovativeness of the CC model[74] and presents a key vulnerability in the cloud environment.[75] The hypervisor is the fundamental component that manages the virtual computing resources and enables the cloud multitenancy environment; it has the highest access rights to the virtual cloud environment.[76] Attacks from the customer organization's insiders, cloud service provider (CSP) insiders, or external attackers are likely to compromise the hypervisor, resulting in full control over the cloud environment and its virtual computing resources.[77]

69. Mell and Grance, 2.
70. Mell and Grance.
71. Ibid.
72. Ibid.
73. Buyya et al.
74. Su et al.
75. Coppolino et al.
76. Ibid.
77. Ibid.

The exploitation of such vulnerability in the cloud environment leads to a forensic cloud problem.[78]

A forensic cloud problem involves attackers being able to gain escalated privileges to access the cloud environment and delete or modify the personal data or settings of the virtual computing resources, as well as delete all traces of their intrusion.[79] In the case of personal data breach, once the attackers delete the audit and forensic data trails to hide the traces of their intrusion, a GDPR compliance issue occurs,[80] because the CSP, as a processor, is unable to notify the controller without undue delay after becoming aware of a personal data breach.[81] Consequently, the customer organization, as a controller, may not be able to notify the personal data breach to the supervisory authority within 72 hours after having become aware of it and without undue delay.[82] When attackers manage to delete these trails, it is difficult for the controller to identify which records have been compromised and whether they have been read, tampered with, or deleted from the cloud storage.[83] Thus, the controller may not be able to notify the supervisory authority of the nature of the personal data breach, the categories and approximate number of the affected data subjects and personal data records, the consequences of the personal data breach, and the measures taken or proposed by the controller to address the personal data breach.[84] As a result, the controller may not be able to comply with the integrity and confidentiality principle of GDPR[85] and may fail to demonstrate that the processing of personal data includes protection against unauthorized processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures.

CC services are offered to the consumers by means of service-level agreements (SLAs) established through a service contract between the service provider and customers.[86] CC service contracts are characterized as toothless; they are weak due to their abstract and standard format and the network

78. Duncan, "Can EU General Data Protection Regulation."

79. Ibid.

80. Duncan and Whittington; Duncan, "Can EU General Data Protection Regulation."; Duncan, "EU General Data Protection Regulation Compliance."

81. Article 33 (2), GDPR.

82. Article 33 (1), GDPR.

83. Duncan, "Can EU General Data Protection Regulation."

84. Article 33 (3), GDPR.

85. Article 5 (1)f, GDPR.

86. Buyya et al.

of third-party CSPs with which the initial CSPs have subcontracts.[87] This leads to compliance issues with GDPR. The negotiated service levels in SLAs are not the same as the actual levels due to the large number of tenants sharing the computing resources; this makes it difficult for the CSPs to provide detailed information and 100% guarantees for equivalent and optimum service levels.[88] Thus, CSPs tend to simplify and standardize their contractual agreements instead of risking the breach of each individual SLA for every single customer and enduring endless penalties.[89] The standard contractual agreement for data transfer from the EU to the United States (EU-US Privacy Shield framework) has been invalidated, due to a recent decision by the CJEU, in July 2020. The grounds for the decision are US Surveillance programs are not limited to necessity and the EU data subjects do not have rights for a compelling remedy in the United States.[90] This will require the US data controllers to conduct a case-by-case detailed analysis of the data transfer surroundings, the sufficiency of protection standards in the country to which the data will be transferred, and the processors involved in processing the data.

In a typical scenario, CSPs may rely on subcontractors. For example, an SaaS CSP may outsource its applications to a PaaS CSP, which may outsource its infrastructure to another IaaS CSP.[91] In their standard agreements, CSPs and their subcontractors tend to be less transparent about the complexity of the cloud infrastructure hardware and details about the location and processing of personal data,[92] and they are still being caught by the EU data protection authorities for their lack of transparency regarding data processing.[93] This puts the initial CSP and its subcontractors out of harmony with GDPR in terms of providing sufficient guarantees to implement appropriate technical and organizational measures to ensure the protection of data subjects' rights.[94] Additionally, it makes it difficult to comply with the contractual requirements under GDPR that stipulate that the CSP, as a processor, and its subcontractors, as subprocessors, shall process

87. El-Gazzar et al.; Lansing and Sunyaev.

88. Venters and Whitley.

89. Ibid; El-Gazzar et al.

90. The Schrems II judgment of the Court of Justice and the future of data transfer regulation: https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation/

91. Russo et al.

92. Altorbaq et al.; Russo et al.

93. Satariano.

94. Article 28 (1) and (4), GDPR.

the personal data as instructed in writing by the customer organization, as a controller.[95] As a result, the controller may not be able to demonstrate transparency of processing the personal data as per the lawfulness, fairness, and transparency principle of GDPR.[96]

The virtual computing and storage resources in a cloud environment are characterized by being geographically distributed to ensure optimum, though not 100%, service availability and data availability through backups.[97] This raises compliance issues with regard to obtaining the data subjects' consent, as IaaS CSPs are inflexible in tailoring their infrastructure for individual customers and it is unclear where the backup copies of the data are located.[98] This makes it difficult for the controller to request consent in a clearly distinguishable manner or to use clear and plain language.[99] Thus, the cloud backup procedures in the context of chained CC subcontractors need to be monitored[100] as they add more concerns regarding the right to erasure. Also, it is challenging to ensure that the backup copies of personal data are deleted from all locations and that the personal data—not just the encryption key of the data—are deleted.[101] This makes it difficult for the controller to comply with the obligation to erase personal data upon request from the data subject without undue delay.[102]

Due to vendor lock-in interoperability problem and that CSPs' use of different application programming interfaces (APIs) and data formats, CC service models raise different levels of flexibility of data portability.[103] Flexibility of data portability increases at the IaaS level and decrease at the SaaS level. The uncertainty regarding the right to data portability[104] stems from the changing role of the CSP as result of its different types of customers (i.e., an organization or a natural person); the CSP becomes a processor when a customer organization is the controller, while the CSP becomes a controller for a natural person.[105] Thus, the CSPs may not be aware of their role as controllers and their responsibility to return

95. Article 28 (3)a, GDPR.
96. Article 5 (1)a, Recital 39, GDPR.
97. Buyya et al.
98. Russo et al.
99. Article 7(2), GDPR.
100. Russo et al.
101. Altorbaq et al.; Politou et al.
102. Article 17(1), GDPR.
103. Wang and Shah.
104. Article 20, GDPR.
105. Wang and Shah.

TABLE 1 CC versus GDPR

CC characteristics	Complies?		GDPR Articles	Justification
	Yes	No		
Virtual cloud environment		X	Article 33 (1), (2), and (3)Article 5(1)f	Attackers can exploit vulnerabilities in the hypervisor and gain escalated privileges to access the cloud environment and delete or modify the personal data or settings of the virtual computing resources, in addition to deleting all the traces for their intrusion, causing a cloud forensic problem. This makes the processor (i.e., CSP) unable to notify the controller without undue delay after becoming aware of a personal data breach. Consequently, the controller (i.e., customer organization) may not be able to notify the personal data breach to the supervisory authority and provide details on the breach within 72 hours after having become aware of it and without undue delay. Thus, the controller may not be able to comply with the "integrity and confidentiality" principle.
Simple and standard CSP contractual agreements		X	Article 28 (1), (3) a, and (4)Article 5 (1)a, Recital 39	The SLAs are not the same as the actual levels due to the large number of tenants; thus, CSPs and their subcontractors tend to provide simple and standard agreements that are less transparent about the complexity of the cloud infrastructure hardware and details about the location and processing of personal data. This does not go in harmony with GDPR in providing sufficient guarantees to implement appropriate technical and organizational measures to ensure the protection of data subjects' rights. It makes it difficult to comply with the contractual requirements under GDPR, where the CSP and its subcontractors shall process the personal data as instructed in writing by the controller. Thus, the controller may not be able to demonstrate transparency of processing the personal data as per the "lawfulness, fairness, and transparency" principle of GDPR

(*Continued*)

TABLE 1 CC versus GDPR (*Continued*)

CC characteristics	Complies?		GDPR Articles	Justification
	Yes	No		
Geographically distributed CC backups		X	Article 7(2)Article 17(1)	It is unclear where the distributed backup copies of personal data are and this makes it difficult to obtain the data subject's consent in clear manner. It also makes it difficult to guarantee the right to erasure and ensure that all the backup copies are deleted.
CC service models		X	Article 20, Article 20(1)Article 15, Article 16, Article 17	The flexibility of data portability increases at the IaaS level and decreases at the SaaS level due to vendor lock-in. The role of CSPs may shift from processor to controller when their customer is a natural person, and they may not be aware of their responsibilities of providing back the personal data to the data subject or another controller based on the data subject's request in a commonly used format without hindrance. CSPs or their customer organizations, as controllers, may not have their data portability mechanisms integrated with methods of access, rectification, and erasure.

personal data to the data subject or transmit them to another controller in a structured, commonly used, and machine-readable format without hindrance.[106] The right to portability may entail guaranteeing the data subject's right of access,[107] right to rectification,[108] and right to erasure.[109] For example, the data subject may request that a controller erase personal data and simultaneously port the data into their own hands or another controller.[110] Controllers, whether they are CSPs or customer organizations, may not have data portability mechanisms integrated with their access, rectification, and erasure methods, which poses a challenge to their compliance with GDPR.

106. Article 20(1), GDPR.
107. Article 15, GDPR.
108. Article 16, GDPR.
109. Article 17, GDPR.
110. Wang and Shah.

BC and GDPR

BC is a sequential distributed database where the entire earlier transaction history is stored and shared in a series of blocks in a public ledger between distributed computers on a network.[111] With every change to a transaction, a new block is created and validated by the participating nodes; if consensus is obtained, the new block is chained to the previous blocks.[112] All transactions are timestamped, and their history is stored permanently and copied to all participants.[113] The main characteristics of BC are transparency, immutability (i.e., a tamper-proof ledger of transaction history), and its deployment models (i.e., public permissionless and private permissioned BCs).[114] Public permissionless BCs have no limits on the number of users who can process and read the transaction data. Private permissioned BCs are limited to a predefined set of known users who process the transactions and read the BC data. Largely, the compatibility between BC and GDPR is determined by the interaction between the BC's technical and contextual characteristics and the GDPR requirements.[115] We summarize our legal analysis of BC and GDPR in Table 2.

The transparency characteristic of BC makes it compatible with GDPR; it manifests the auditable distributed ledger of transaction data and history that is shared between all participants in the BC (i.e., individuals or other body having controller or processor responsibilities or both) in an easy to access manner.[116] This makes BC compatible with the GDPR principle of lawfulness, fairness, and transparency,[117] where the transparency requires that any information and communication relating to the processing of personal data shall be easily accessible and easy to understand and that clear and plain language be used to ensure fairness and transparency.[118] The transparency of BC improves the accountability by tracking all the transactions,[119] which enables compliance with the accountability principle under GDPR.[120] However, public permissionless BCs are more transparent than

111. Lindman et al.; Halaburda; Underwood.
112. Korpela et al.; Swan.
113. Alexopoulos et al.
114. Ibid; Underwood; Makhdoom et al.
115. Finck.
116. EU; Finck.
117. Article 5(1), GDPR.
118. Article 5, Recital 39, GDPR.
119. EU.
120. Article 5(2), GDPR.

private permissioned BCs[121] due to their read and processing restrictions on the blocks.[122]

The issue between BC and GDPR is its immutability, meaning that the data can never be altered or deleted. The large number of participating nodes in the public permissionless BC makes it more difficult to alter than the private permissioned BC, as changes and deletions to transactions that are already added to the BC are difficult to apply.[123] The immutability of public permissionless BCs conflicts with the right to erasure[124] and the right to rectify incorrect data[125] given to data subjects under GDPR.[126] To address the right to rectify, research suggests that a new block can be added containing the update transaction to personal data, while not modifying the old block that contains the old or incorrect personal data.[127] This implies that the old or incorrect personal data still exists, which could lead to the low data quality and redundancy of data.

Private permissioned BCs can allow for deleting and altering personal data, as they involve a limited number of trusted participating nodes that are created, run, and controlled by governance authority.[128] In this scenario, the governance authority represents the data controller and would still have multiple data processing agreements with the created nodes.[129] In the private permissioned BCs, the right to erasure and to rectify can be maintained since the data controller(s) with governance and creation authority over the data processor nodes can alter or delete the personal data, and the other processor nodes would then follow the same action.[130]

BC's ever-growing immutable ledger of transaction history,[131] especially in public permissionless BCs, raises a concern regarding the storage limitation principle of GDPR,[132] which states that personal data shall be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

121. EU; Landerreche and Stevens.
122. Walsh et al.; Hans et al.; Underwood.
123. van Geelkerken and Konings.
124. Article 17, GDPR.
125. Article 16, GDPR.
126. Hawig et al.
127. van Geelkerken and Konings.
128. Ibid.
129. Ibid.
130. Ibid.
131. Underwood.
132. Article 5(1)e, GDPR.

TABLE 2 BC versus GDPR

BC characteristics	Complies?		GDPR Articles	Justification
	Yes	**No**		
Transparency and public permissionless BC/ private permissioned BC	X		Article 5 (1), (2), Recital 39	Public permissionless BCs are transparent, as there are not limitations on who reads and processes the blocks in the distributed ledger of transaction data and history that is shared between all participants. This makes BC compatible with the GDPR principle of lawfulness, fairness, transparency, as well as accountability principle by tracking all the transactions.
		X		Private permissioned BCs are less transparent due to their read and processing restrictions on the blocks.
Immutability and public permissionless BC/private permissioned BC	X		Article 16 Article 17 Article 5 (1)e Article 5 (1)c	Private permissioned BCs can allow the deleting and altering of personal data, as they involve a limited number of trusted participating nodes controlled by a governance authority. Thus, the right to erasure and the right to rectify can be maintained since the controller(s) with governance and creation authority over the data processor nodes can alter or delete the data.
		X		• The large number of participating nodes in the public permissionless BC makes it difficult to alter, which conflicts with the right to erasure and the right to rectify incorrect data. • The ever-growing immutable ledger of transaction history in public permissionless BCs conflicts with the data minimization and storage limitation principles of GDPR.

At the same time, the growing immutable ledger of public permissionless conflicts with the data minimization principle of GDPR,[133] which states that adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. Private permissioned BCs allow for the deletion of personal data after a period of time.[134] A proposal for a forgetting BC relied on private permissioned BC, where any existing block can be deleted after a predefined amount of time to allow for the deletion effect to be synchronized in all nodes in the BC.[135] This proposed forgetting BC has limitations regarding the maintenance of the links between the remaining blocks in the BC after a particular block is deleted.[136]

It is claimed by researchers that the right to erasure[137] by GDPR can be addressed in public permissionless BC through pseudonymization, where the transaction data is encrypted with a secret key and the key remains with the controller for later reidentification of the data.[138] However, to erase the data, the secret key can be deleted so that the data could not be reidentified again.[139] This way, the data would no longer be identifiable, which would comply with the right to erasure. Such a proposal strengthens the immutability of the BC and fulfills the right to erasure by GDPR, which requires the data to be nonexistent and irretrievable.

IoT and GDPR

IoT offers a variety of values to organizations and nations, such as increasing productivity, improving quality of life, process automation, personalization of services, context-specific applications, and real-time generation of rich data.[140] However, there are major issues that affect the realization of those values, including privacy, security attacks, interoperability as a result of device heterogeneity, technological immaturity in storing and processing massive amount of data, and inadequate regulatory frameworks.[141]

133. Article 5(1)c, GDPR.
134. Gilbert.
135. Farshid et al.
136. Ibid.
137. Article 17, GDPR.
138. Hawig et al.
139. van Geelkerken and Konings.
140. Papadopoulou et al.
141. Ibid.

We use the definition of IoT by Gubbi et al.[142] as it provides the following context about the technical characteristics:

> [IoT is the] interconnection of sensing and actuating devices providing the ability to share information across platforms through a unified framework, developing a common operating picture for enabling innovative applications. This is achieved by seamless ubiquitous sensing, data analytics and information representation with cloud computing as the unifying framework.

The core elements of IoT, as stated by Gubbi et al.[143] are the hardware components (i.e., sensors, actuators, and embedded communication devices, such as RFID, cloud-based storage and computing resources to perform big data analytics, and visualization and interpretation tools that can be accessed on different platforms and used by different applications.

According to Article 29 Data Protection Party ("WP 29"), IoT involves extensive processing of a massive amount of data collected on identifiable natural persons through sensors and processes this data to analyze the individual's environment or behavior.[144] This invasive profiling of natural persons within the IoT environment is intended to provide those persons with personalized services and experiences. Furthermore, many stakeholders are involved in the processing of these voluminous personal data, including device manufacturers—that sometimes also act as data platforms, data aggregators, or brokers—application developers, social platforms, device owners, or renters.

The major issues between IoT and GDPR are about transparency, consent, privacy, discrimination, and complex contractual relationships (see summary in Table 3). IoT is characterized by the use of identification technologies to constantly link data from the individuals' devices to their unique identities in addition to linking data between devices and services to provide them with personalized services.[145] Individuals may not be informed about this constant identification and data linkage as it happens[146] as it is difficult to gain explicit consent from the data subject for

142. Gubbi et al., 1647.

143. Gubbi et al.

144. WP29, Opinion 8/2014, page 4.

145. Wachter, "Normative Challenges of Identification."; Wachter, "The GDPR and the Internet of Things."

146. Wachter, "Normative Challenges of Identification."

each IoT device connected to the IoT environment.[147] In addition to not being aware of how their personal data are collected by, shared with, and further processed by IoT devices, data subjects may not be informed about many stakeholders and third parties involved in the processing of their personal data and recipients with whom personal data may be shared.[148] This complex scenario makes it difficult for controllers to comply with their obligations under GDPR to inform the data subjects about the collection of their personal data, and transparency may be lacking with regard to the processing of their personal data that may take place between the IoT devices or the involved stakeholders and recipients.[149] As a result, data subjects are unable to freely give their "specific, informed, and unambiguous" consent "by a statement or by a clear affirmative action" indicating their agreement to the processing of their personal data,[150] which makes the data processing unlawful.[151]

IoT is characterized by the collection of voluminous personal data, which likely consists of more information than is necessary, from the data subjects or sensors in IoT devices by automated invasive tracking of data subjects' behavior.[152] Additionally, controllers may draw inferences about the data subject that are not related to the purpose for which the data was collected and of which the data subject is not aware.[153] Likewise, third parties involved in the processing of personal data may use the data for other purposes of which the data subject is not aware.[154] This does not comply with the data minimization principle of GDPR, which stipulates that the data shall be relevant and limited to what is necessary in relation to the purposes they are collected for.[155] If controllers minimize the amount of personal data collected by IoT devices, they will comply with GDPR, but the IoT services will not function properly,[156] which implies that the business model for using IoT services is no longer sufficient if personal data collection is minimized. Furthermore, drawing inferences for purposes other

147. Vegh.

148. Wachter, "Normative Challenges of Identification."

149. Article 12 (1), Article 13, and Article 14 (1-4), GDPR.

150. Article 4 (11), GDPR.

151. Article 6 (1)a, GDPR.

152. Wachter, "Normative Challenges of Identification."; Wachter, "The GDPR and the Internet of Things."

153. Wachter, "Normative Challenges of Identification."

154. Ibid.

155. Article 5 (1)c, GDPR.

156. Wachter, "Normative Challenges of Identification."

than the intended data collection purpose and without the data subject's consent conflicts with the purpose limitation principle of GDPR.[157]

IoT is also characterized by the application of big data analytics and complex algorithms to make invasive profiling inferences about the data subject by linking IoT datasets or combining datasets shared by third parties.[158] In this scenario, the controllers may invade the privacy of the data subject by combining multiple categories of data without the data subject's knowledge.[159] Additionally, IoT-drawn inferences for personalization purposes may lead to discriminatory treatment of the data subject.[160] If data subjects are not aware of the invasive profiling by the controller and third parties, they will be unable to exercise their right not to be subject to a decision based solely on automated processing, including profiling that has legal and significant impact on them.[161] Further inferences by third parties without informing the data subject will conflict with their right, under GDPR, to be informed about the existence of automated decision-making, including profiling, and meaningful information about the logic involved.[162] Additionally, providing meaningful information about the logic of big data analytics and complex algorithms to data subjects to comply with GDPR may not be a simple obligation for the controller to fulfill. Furthermore, personalization resulting from IoT profiling inferences that lead to discriminatory treatment to the data subject may clash with the fairness principle of GDPR.[163]

In the context of IoT, contractual agreements that manage relationships between stakeholders involved in processing personal data are characterized as multilayered and complex.[164] Complexity manifests in defining the roles of controllers, processors, and subprocessors, as well as distributing data processing responsibilities and formal obligations between the multilayered IoT stakeholders.[165] In the context of IoT, controllers' in-house capabilities for housing IoT devices and storing the massive amount of data collected by IoT devices, communication infrastructure, and processing

157. Article 5 (1)b, GDPR.

158. Wachter, "Normative Challenges of Identification."; Wachter, "The GDPR and the Internet of Things."

159. Wachter, "Normative Challenges of Identification."

160. Ibid.

161. Article 22, GDPR.

162. Article 13 (2)f and Article 14 (2)f, GDPR.

163. Article 5 (1)a, GDPR.

164. Lindqvist.

165. Ibid.

TABLE 3 IoT versus GDPR

IoT characteristics	Complies?		GDPR Articles	Justification
	Yes	No		
Constant identification, data linkage, IoT devices, and multiple stakeholders		X	Article 12 (1), Article 13, Article 14 (1–4), Article 4 (11), Article 6 (1)a	Data subjects may not be aware of the constant identification of the data subjects by IoT devices, data linkage between IoT devices, data collection and sharing between IoT devices, and data processing by IoT devices and many stakeholders. This makes it difficult for the controllers to inform the data subjects of the collection and processing of their personal data. Thus, data subjects may not be able to give an informed consent regarding the processing of their personal data.
Excessive data collection, change of processing purpose by third parties		X	Article 5 (1)c, Article 5 (1)b	Collecting voluminous personal data about the data subjects and their behavior more than necessary. Controllers and third parties may process the massive personal data they collected for other purposes than the collection purpose without the data subjects being aware of that.
big data analytics, algorithms, and multiple stakeholders		X	Article 22, Article 13 (2)f, Article 14 (2)f, Article 5 (1)a	Data subjects may not be aware of the invasive profiling done by the controller and third parties through big data analytics and algorithms. This conflicts with the obligation on the controllers to inform the data subjects of the existence of automated profiling mechanisms and the processing logic of the big data analytics and algorithms used. Thus, data subjects unable to exercise their right not to be subject to automated profiling that may have legal and significant impact on them. Profiling for the purpose of personalizing the services to data subjects leads to an unfair processing.
Connected IoT devices, big data analytics and algorithms, and complex multilayered contractual relationship between IoT stakeholders		X	Article 28 (3), Article 5 (2)	In reality, the processors are the ones who draft the contractual terms and processing instructions. This reverses the obligation put on the controller to provide the processor with the processing instructions. This also may have the controller unable to demonstrate accountability, as the standard contracts of the processors and their subprocessors may not be detailed as required by GDPR. It also becomes difficult to demonstrate accountability for the damage caused to the data subjects by IoT devices or big data analytics and algorithms.

operations (i.e., big data analytics functionalities, inferencing algorithms, and visualization tools) are limited. Thus, a typical IoT environment consists of controllers relying on manufacturers to provide them with IoT devices and outsourcing the processing operations and communication infrastructure to several initial processors (e.g., CSPs offering SaaS services for big data analytics) who may already be relying on subprocessors (e.g., third-party CSPs offering IaaS services for storing data).

This multilayered contractual relationship raises compliance issues with Article 28 of GDPR, which stipulates the obligations of the controller regarding the choice of processors and entering into agreements with subprocessors, as well as the detailed elements that the data processing contract shall include.[166] Among those elements, the processor shall process the personal data "only on documented instructions from the controller."[167] However, in reality, the processors are the ones who draft standard contractual terms and processing instructions because they process data on behalf of many controllers and do not have separate processing instructions for each controller.[168] This makes it difficult for the controllers to comply with the contractual requirements[169] and the accountability principle under GDPR,[170] as they are not fully aware of all of the processors and subprocessors involved.[171] Furthermore, the complex multilayered contractual relationships between IoT stakeholders make it more difficult to claim the responsibility for a damage caused to data subjects by IoT devices or analytical algorithms.[172]

AI and GDPR

AI systems are open autonomous systems that can learn, adapt to the surroundings, and make conclusions and decisions based on analyzing big data about different situations without human intervention.[173] Kaplan and Haenlein[174] defined AI as "a system's ability to interpret external data

166. Article 28, GDPR.
167. Article 28 (3)a, GDPR.
168. Lindqvist.
169. Article 28 (3), GDPR.
170. Article 5 (2), GDPR.
171. Lindqvist.
172. Ibid.
173. Sousa et al.
174. Kaplan and Haenlein.

correctly, to learn from such data, and to use those learnings to achieve specific goals and tasks through flexible adaptation." AI systems take inputs from IoT devices as sources of big data to identify patterns using ML algorithms.[175] Based on big data analytics and pattern identification, AI systems are able to predict the future behavior of humans.[176] AI systems are characterized by automation and autonomy in developing perception and cognition of relevant aspects of their surrounding environment (i.e., inferences), and they have goals, make decisions, and take actions toward achieving those goals.[177] AI systems are classified into analytical AI, human-inspired AI, and humanized AI.[178] Analytical AI systems have cognitive intelligence characteristics as they can generate a cognitive image of the world and incorporate past experience to make informed decisions (e.g., systems used for fraud detection in financial services, image recognition, or self-driving cars). Human-inspired AI systems have cognitive emotional intelligence characteristics as they understand human emotions (e.g., joy, sadness, anger) and consider them in making their decisions. Humanized AI systems exhibit cognitive, emotional, and social intelligence characteristics (e.g., robot Sophia[179]).

AI has been overhyped with superficial marketing to promote the notion of "machines think, decide, and do" instead of "machines do".[180] This marketing hype conveys an artificial understanding of AI systems to potential users from individuals and organizational users and falls short of informing them of the ethical and legal consequences from using those systems.[181] The ethical and legal issues concerning AI are not well addressed in previous research and can have negative implications for actual and potential adopters.[182] The use of ML algorithms and big data analytics in modern data processing techniques requires a different approach by controllers in order to comply with GDPR; this approach must focus on ethical values rather than only data quality and security.[183] We summarize our legal analysis of AI and GDPR in Table 4.

175. Ibid.
176. Sousa et al.
177. Clarke.
178. Kaplan and Haenlein.
179. CNBC.
180. Clarke.
181. Ibid.; Mantelero.
182. Sousa et al.; Butterworth.
183. Mantelero; Weber.

The conflict between AI and GDPR manifests in the autonomy of AI systems, leading to compliance issues with the accountability principle of GDPR.[184] This raises the question: "Can an AI system enter into data processing agreements and interact with individuals and data controllers without intervention from its owner, [and] would the owner still be liable for the decisions made and actions taken by the AI system?".[185] It is unclear whether AI systems are considered controllers or processors.[186] AI systems may make unreasonable inferences and decisions and take harmful actions, which may have harmful impacts on human life, as well as lead to unfair and unappealable decisions by legal authorities regarding penalties.[187] It has been suggested that AI systems should be treated as human citizens with ethical rights and legal obligations so that they can be held accountable for processing misconduct.[188]

AI systems, whether they are built on theoretical or empirical bases, are characterized as multilayered systems with complex ML algorithms and logics used to automate the processing of personal data and decision-making; thus, it becomes difficult to explain the inferences, decisions, and actions of those systems.[189] The difficulty in explaining the data processing and decision-making logics of AI systems raises transparency compliance issues regarding the processing of personal data under GDPR.[190] GDPR requires controllers to provide the data subject with information about the existence of automated decision-making, including profiling to ensure fair and transparent processing. The data subject has the right to access such information and further meaningful information about the logic involved in processing the personal data, as well as significant and expected consequences of such processing for the data subject.[191] This may raise concerns regarding the data subject's right not to be subject to a decision based solely on automated processing, including profiling, which significantly affects him or her.[192]

184. Article 5 (2), GDPR
185. Butterworth, 258.
186. Butterworth.
187. Sousa et al.; Clarke.
188. Butterworth.
189. Clarke.
190. Ibid.
191. Articles 13 (2)f, 14 (2)g and 15 (1)h, GDPR.
192. Article 22 (1), GDPR.

Although GDPR does not explicitly require controllers to ensure privacy policy, the obligations imposed on the controllers to provide data subjects with information about the processing of their personal data[193] indirectly requires them to create one.[194] Furthermore, a well-designed privacy policy has to be comprehensive, including all information required in a clear language about fair and unlawful processing so that the data subjects can understand all aspects of processing their personal data and exercise their rights under GDPR.[195] Thus, the power of AI and ML algorithms can help controllers conduct an automated legal analysis of the privacy policies of their online platforms and services and refine those policies to comply their information obligations under GDPR.[196] Moreover, the majority, if not all, of privacy policies are long and difficult for data subjects to read and understand, making it difficult for them to be informed about the processing activities that may take place on their personal data so that they can make informed decisions with regard to giving their personal data.[197] ML algorithms may be used to automatically summarize controllers' privacy policies to enable data subjects to exercise their rights to be informed about data processing activities under GDPR and, thus, make informed decisions regarding the disclosure of their personal data.[198]

ML algorithms may produce discriminatory results, as the training data fed into the algorithms may provide a biased representation of the reality, which clashes with the fairness principle of processing personal data under GDPR.[199] This manifests in automated decision-making, including profiling[200] that emphasizes racial, political, religious, health status, or sexual data in the data training model and can lead to the discriminatory treatment of the data subjects.[201]

The use of ML algorithms brings compliance issues with the purpose limitation principle of GDPR,[202] which stipulates that personal data shall be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. ML

193. Articles 12, 13, and 14, GDPR.
194. Contissa et al.
195. Ibid.
196. Ibid.; Restrepo Amariles et al.
197. Tesfay et al.
198. Ibid.
199. Article 5 (1)a, GDPR.
200. Butterworth.
201. Datatilsynet.
202. Article 5 (1)b, GDPR.

TABLE 4 AI versus GDPR

AI characteristics	Complies?		GDPR Articles	Justification
	Yes	No		
Autonomy		X	Article 5 (2)	It makes it difficult to hold AI systems accountable for the harm they may cause to the data subject.
Automation and ML algorithms		X	Article 13 (2)f, Article 14 (2)g, Article 15 (1)h, Article 22 (1)	It makes it difficult to explain the complex ML algorithm logics used to process the personal data undermines fairness and transparency of processing. Thus, the data subjects are unable to choose not to be subject to automated decision-making and profiling, as they do not know the consequences of it on them.
	X		Article 12, Article 13, Article 14	1) It enables controllers to conduct an automated legal analysis, using ML algorithms, of the privacy policies of their online platforms and services and refine them to, indirectly, comply with their information obligations under GDPR. 2) It enables automatic summarization of the controllers' privacy policies, so that data subjects can exercise their rights to be informed about data processing activities and make informed decisions about disclosing their personal data.
		X	Article 5 (1)a	3) ML algorithms may produce results that are discriminatory because the training data provides a biased representation of the reality, which indicates unfair processing of the personal data.
ML algorithms and big data		X	Article 5 (1)b	ML algorithms may process personal data for ambiguous and illegitimate purposes and generate new data, which makes it unclear for data subjects what will be the purpose for using all these data.
		X	Article 5 (1)c	ML algorithms tend to collect big personal data and repurpose them, which makes it unclear for data subjects if all these data are adequate and relevant for the purpose they are processed for.
		X	Article 4 (11)	Processing and repurposing big personal data make it difficult to obtain an informed consent based on a statement or a clear affirmative action.

algorithms may process personal data for other ambiguous purposes than those the data have been initially collected for and generate new types of data; thus, the purpose that the data will be used for remains unclear to the data subjects.[203]

ML algorithms tend to collect and process big personal data and repurpose them,[204] clashing with the data minimization principle of GDPR, which requires personal data to be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.[205] Moreover, processing and repurposing big personal data makes it difficult to obtain an "informed and unambiguous" consent from data subjects "by a statement or by a clear affirmative action," as required by GDPR.[206]

Discussion and Conclusion

CC, BC, IoT, and AI represent the future trends for public and private sectors; however, these four emerging technologies are at different level of maturity and face serious challenges since GDPR came into effect. In this article, we examined compliance challenges brought to these technologies by GDPR. To revisit, we aimed to answer the following research question: How does GDPR challenge the nature of emerging technologies? To do this, we conducted a legal analysis of the characteristics of each individual technology against the formal articles of GDPR. In our analysis, we relied on evidence from previous studies as examples for our arguments. Our analysis resulted in identifying compliance challenges as well as opportunities with GDPR for each technology. From our analysis, we summarize the results of our analysis and possible outlooks into the following points of discussion:

1. **The characteristics of each technology are challenged for their compliance with GDPR, but the context of use creates opportunities for compliance with GDPR**

   The natural characteristics of the emerging technologies are challenged by GDPR, as they emerged before the development of GDPR.[207]

203. Butterworth.
204. Ibid.
205. Article 5 (1)c, GDPR.
206. Article 4 (11), GDPR.
207. Pham; Bastos et al.

Therefore, the characteristics of each technology raise compliance issues with GDPR, its principles, and data subject rights. For CC, the analyzed characteristics are the virtual cloud environment, simple and standard SLAs, geographically distributed backups, and CC services models. All the characteristics of CC are found to be challenged by GDPR. Similarly, all the analyzed characteristics of IoT are challenged by GDPR. These characteristics are IoT devices and their excessive data collection, constant identification, data linkage, change of processing purposes by third parties, big data analytics and algorithms, as well as the multiple IoT stakeholders and the complex contractual relationships between them.

From our analysis of BC and AI, we find that the context of using the technology determines its compliance. The analyzed characteristics of BC are transparency, immutability, and its deployment models, where public permissionless BCs outperform private permissioned BCs in transparency requirements under GDPR; thus, show compliance with GDPR. Regarding immutability, unlike public permissionless BCs, alteration and deletion can be done to private permissioned BCs, which makes them compliant with the right to erasure. The analyzed characteristics of AI are autonomy, automation, ML algorithms, and big data. While the majority of AI characteristics are challenged for their compliance with GDPR, the different contexts of using automation and ML algorithms may offer opportunities or pose compliance challenges. When ML algorithms are used for conducting legal analysis of privacy policies of online platforms, they offer opportunities for ensuring compliance with information obligations under GDPR. However, when automation and ML algorithms are used for generating inferences from personal data collected from the data subjects, they pose compliance challenges with GDPR. The complex ML algorithms of AI make it difficult to explain the processing logic, which undermines the transparency required under GDPR.

2. Possible approaches to address the compliance challenges with GDPR

Two approaches can address the compliance challenges brought by GDPR to the natural characteristics of the four emerging technologies. One approach is to combine any of the four technologies so that the characteristics of one technology addresses the compliance challenges in the other. The other approach is requirements engineering for GDPR compliance by design, which is concerned about software design, development, and operations.

TABLE 5 Combinations of technologies versus GDPR

CC	BC	IoT	AI	Comply?		GDPR Articles	Justification
				Yes	No		
X	X			X		Article 33 (1), (2), and (3)	BC addresses the CC forensic problem through its immutability characteristic, so that the history of all transactions and activities within the cloud environment is persistent and traceable. This makes it difficult for the attacker to tamper with the transactions data, because the larger the number of blockchain nodes the more difficult to alter the data.[208]
X		X			X	Article 33 (1), (2), and (3)	1) IoT increases the cloud forensic problem due to IoT devices have limited memory capacity and can be exploited by the attackers to access the cloud's virtual environment and gain access to sensitive data.[209] 2) Personal data are collected and processed by IoT devices from different manufacturers and not directly by the cloud providers and IoT devices may have internal storage utilities embedded by the manufacturers; thus, there is not enough information about where the data are being stored geographically in the cloud environment and physically in the IoT devices.[210]
	X	X		X		Article 5(2)	BC can be used to design GDPR-based smart contracts that are privacy aware to improve the accountability of IoT devices, which are data controllers or processors of user data.[211]
	X		X	X		Article 22(3) and (4)	Storing sensitive data on a BC, which can be accessed by an AI, but only with permission and once it has gone through the proper procedures, could give enormous advantages of personalized recommendations while safely storing personal sensitive data.[212]

208. Makhdoom et al.; Zhao and Duncan.
209. Duncan and Zhao.
210. Atzori et al.; Bastos et al.
211. Barati et al.
212. Banafa.

The approach of combining the technologies may solve compliance challenges with GDPR; however, it may complicate these challenges in some occasions (see Table 5 for more examples). For example, the virtual cloud environment has a forensic problem that brings compliance issues regarding the obligation to notify the supervisory authority about data breach within 72 hours; the immutability of BC addresses the cloud forensic problem, although the immutability has compliance issues with the right to erasure under GDPR.

The opposite case of complicating compliance challenges manifests in combining CC and IoT. CC is the infrastructure technology for IoT that enables storing and processing the vast amount of data generated from different IoT devices.[213] This takes the compliance issues related to CC to a higher level of complexity given that personal data are collected and processed by IoT devices from different manufacturers and not directly by the cloud providers.[214] In addition, IoT devices may have internal storage utilities embedded by the manufacturers, further increasing the complexity.[215] The right to erasure becomes difficult to maintain in the IoT environment, as there is no transparency on how the data are collected, analyzed, and stored.[216] The complexity of the data storage is even problematic with IoT because there is not enough information about where the data are being stored geographically in the cloud environment and physically in the IoT devices that have storage capabilities as well.

The second approach is concerned about fulfilling GDPR compliance by design; it aims at requirements engineering and redesigning of information systems and services for the emerging technologies.[217] This approach is in harmony with the GDPR requirements to implement appropriate technical and organizational measures for ensuring that, by default, only personal data that are necessary for each specific purpose of the processing are processed.[218] The approach to GDPR compliance by design has four design principles[219]: redesigning the software to the Data Protection Officer's (DPO) technical needs and organizational demands, designing data protection measures to enable monitoring and control of data

213. Atzori et al.
214. Ibid; Shim et al.
215. Atzori et al.
216. Bastos et al.
217. Tamburri.
218. Article 25(2), GDPR.
219. Article 25, GDPR.

processing, designing appropriate rules for processing multiple data-levels, and increasing awareness and training.[220] Such GDPR compliance by design cannot be achieved without a close cooperation and collaboration of a wide range of stakeholders including managers, DPO, software engineers, and software designers.[221] However, stakeholders may vary depending on the type of organization that adopts any emerging technology and dealing with GDPR compliance, which offers opportunities for future research.

However, this approach has two drawbacks. First, the attempt to make a technology comply with GDPR may hinder its intended functionalities. For example, in the pure nature of BC, old blocks cannot be deleted; however, new blocks can be added to show any changes in the data stored. This feature is challenged by GDPR, which gives data subjects the right to erasure.[222] Therefore, if BC characteristics are redesigned to meet this GDPR requirement, will it still operate as intended? This question can also be applied to CC, IoT, and AI since the fundamental characteristics of these technologies do not comply with GDPR.[223]

Second, GDPR is written by lawyers and policy-makers, and not by software engineers; additionally, there is little effort from scholars to investigate GDPR for the benefit of practitioners involved in the system development life cycle (SDLC) and most of the researchers focused on policy and business perspectives regarding the compliance with GDPR.[224] Thus, practitioners involved in the SDLC of software for the emerging technologies may face challenges in fulfilling GDPR compliance by design. Therefore, there is a need to investigate the ramifications of GDPR on the further development of this technology as well as to question: how will emerging technologies protect our privacy in the future?

At the best, GDPR compliance by design is the short-term solution to the compliance challenges to the four emerging technologies. In the long term, the adaptation of the EU data protection law may take place to accelerate the adoption of the emerging technologies. We have witnessed the revision of the EU data protection law from Directive 95/46/EC to GDPR in order to accommodate the use of new technologies and facilitate

220. Tamburri.
221. Ibid.
222. van Geelkerken and Konings.
223. Altorbaq et al.; Wachter.
224. Tamburri.

the exchange of personal data across borders.[225] As much as GDPR may be seen as a hassle to many organizations, it has helped increasing awareness of data use and abuse in the very digitally connected world we live in. It remains to be seen how emerging technologies will influence future data protection regulations.

REFERENCES

Achmat, Luqman, and Irwin Brown. "Artificial Intelligence Affordances for Business Innovation: A Systematic Review of Literature." *Proceedings of the 4th International Conference on the Internet, Cyber Security and Information Systems* 12 (2019): 1–12.

Alexopoulos, Charalampos, et al. "Benefits and Obstacles of Blockchain Applications in E-Government." *Proceedings of the 52nd Hawaii International Conference on System Sciences*, Maui, HI, ScholarSpace, 2019.

Altorbaq, Alaa, Fredrik Blix, and Stina Sorman. "Data Subject Rights in the Cloud: A Grounded Study on Data Protection Assurance in the Light of GDPR." *2017 12th International Conference for Internet Technology and Secured Transactions (ICITST 2017)*, Cambridge, UK, IEEE, 2017.

Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "Understanding the Internet of Things: Definition, Potentials, and Societal Role of a Fast Evolving Paradigm." *Ad Hoc Networks* 56 (2017): 122–40.

Avital, Michel, et al. "Jumping on the Blockchain Bandwagon: Lessons of the Past and Outlook to the Future." *Proceedings of the 37th International Conference on Information Systems*, Dublin, Ireland, Association for Information Systems, 2016.

Banafa, Ahmed. "Blockchain and AI: A Perfect Match?" *OpenMind BBVA*. 2019. https://www.bbvaopenmind.com/en/technology/artificial-intelligence/blockchain-and-ai-a-perfect-match/.

Barati, Masoud, Ioan Petri, and Omer F. Rana. "Developing GDPR Compliant User Data Policies for Internet of Things." *Proceedings of the 12th IEEE/ACM International Conference on Utility and Cloud Computing*, Auckland, NZ, IEEE, 2019.

Bastos, Daniel, et al. "GDPR Privacy Implications for the Internet of Things." *4th IoT Security Foundation Conference*, London, UK, IoT Security Foundation, 2018.

Burri, Mira, and Rahel Schär. "The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy." *Journal of Information Policy* 6, no. 2016 (2016): 479–511.

Butterworth, Michael. "The ICO and Artificial Intelligence: The Role of Fairness in the GDPR Framework." *Computer Law and Security Review* 34, no. 2 (2018): 257–68. https://doi.org/10.1016/j.clsr.2018.01.004.

Buyya, Rajkumar, et al. "Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility." *Future Generation Computer Systems* 25, no. 6 (2009): 599–616.

Clarke, Roger. "Why the World Wants Controls over Artificial Intelligence." *Computer Law & Security Review* 35, no. 2019 (2019): 423–33.

225. Burri and Schär.

CNBC. "Humanoid Robot Sophia—Almost Human or PR Stunt." YouTube video, 10:27. Posted by CNBC, June 5, 2018. www.youtube.com/watch?v=7fnCQC7bLs0.

Contissa, Giuseppe, et al. "Claudette Meets GDPR: Automating the Evaluation of Privacy Policies Using Artificial Intelligence." Available at SSRN 3208596, 2018..

Coppolino, Luigi, et al. "Cloud Security: Emerging Threats and Current Solutions." *Computers and Electrical Engineering* 59, no. 2017 (2017): 126–40.

Datatilsynet. "Artificial Intelligence and Privacy." https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf.

De Magalhães Santos, Larissa Galdino. "Towards the Open Government Ecosystem: Open Government Based on Artificial Intelligence for the Development of Public Policies." *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age,* Delft, the Netherlands 2018.

Dorri, Ali, Salil S. Kanhere, and Raja Jurdak. "Towards an Optimized BlockChain for IoT." *Proceedings of the Second International Conference on Internet-of-Things Design and Implementation (IoTDI '17)*, Pittsburgh, PA, IEEE, 2017.

Duncan, Bob. "Can EU General Data Protection Regulation Compliance Be Achieved When Using Cloud Computing?" *Proceedings of the Ninth International Conference on Cloud Computing, GRIDs, and Virtualisation (CLOUD COMPUTING 2018)*, Barcelona, Spain, IARIA, 2018.

———. "EU General Data Protection Regulation Compliance Challenges for Cloud Users." *Proceedings of the Tenth International Conference on Cloud Computing, GRIDs, and Virtualization (CLOUD COMPUTING 2019)*, 2019: 232–242.

Duncan, Bob, and Mark Whittington. "The Complexities of Auditing and Securing Systems in the Cloud—Is There a Solution and Will the GDPR Move It up the Corporate Agenda?." *International Journal on Advances in Security* 11, no. 3 and 4 (2018).

Duncan, Bob, and Yuan Zhao. "Cloud Compliance Risks." *The Tenth International Conference on Cloud Computing, GRIDs, and Virtualization (CLOUD COMPUTING 2019)*, Venice, Italy, IARIA, 2019.

El-Gazzar, Rania, Eli Hustad, and Dag H. Olsen. "Understanding Cloud Computing Adoption Issues: A Delphi Study Approach." *Journal of Systems and Software* 118 (2016): 64–84. https://doi.org/10.1016/j.jss.2016.04.061.

EU. "What If Blockchain Offered a Way to Reconcile Privacy with Transparency?" 2018. https://www.europarl.europa.eu/RegData/etudes/ATAG/2018/624254/EPRS_ATA(2018)624254_EN.pdf.

EUR-Lex. "General Data Protection Regulation." *Official Journal of the European Union*. 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1374-1-1 (accessed February 1, 2020).

Farshid, Simon, Andreas Reitz, and Peter Roßbach. "Design of a Forgetting Blockchain: A Possible Way to Accomplish GDPR Compatibility." *Proceedings of the 52nd Hawaii International Conference on System Sciences*, Maui, HI, ScolarSpace, 2019.

Finck, Michèle. "Blockchain and the General Data Protection Regulation Can Distributed Ledgers Be Squared with European Data Protection Law?" 2019. https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf.

Gilbert, Francoise. "GDPR and blockchain: can they coexist?." 2018. https://www.expertguides.com/articles/gdpr-and-blockchain-can-they-coexist/ARTKQOPD.

Gobeo, A, C. Fowler, and W. J. Buchanan. *GDPR and Cyber Security for Business Information Systems*, Gistrup Denmark: River Publishers, 2018.

Gubbi, Jayavardhana, et al. "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions." *Future Generation Computer Systems* 29, no. 7 (2013): 1645–60.

Halaburda, Hanna. "Economic and Business Dimensions: Blockchain Revolution without the Blockchain?" *Communications of the ACM* 61, no. 7 (2018): 27–29.

Hans, Ronny, et al. "Blockchain and Smart Contracts: Disruptive Technologies for the Insurance Market." *Proceedings of Twenty-Third Americas Conference on Information Systems (AMCIS 2017)*, Boston, MA, Association for Information Systems, 2017.

Hawig, David, et al. "Designing a Distributed Ledger Technology System for Interoperable and General Data Protection Regulation-Compliant Health Data Exchange: A Use Case in Blood Glucose Data." *Journal of Medical Internet Research* 21, no. 6 (2019): e13665. https://doi.org/10.2196/13665.

Herian, Robert. "Regulating Disruption: Blockchain, GDPR, and Questions of Data Sovereignty." *Journal of Internet Law* 22, no. 2 (2018): 8–16.

Kaplan, Andreas, and Michael Haenlein. "Siri, Siri, in My Hand: Who's the Fairest in the Land? On the Interpretations, Illustrations, and Implications of Artificial Intelligence." *Business Horizons* 62, no. 1 (2019): 15–25. Elsevier Ltd..

Korpela, Kari, Jukka Hallikas, and Tomi Dahlberg. "Digital Supply Chain Transformation toward Blockchain Integration." *Proceedings of the 50th Hawaii International Conference on System Sciences* 41 (2017): 82–91.

Kshetri, Nir. "Privacy and Security Issues in Cloud Computing: The Role of Institutions and Institutional Evolution." *Telecommunications Policy* 37, no. 4–5 (2013): 372–86.

Landerreche, Esteban, and Marc Stevens. "On Immutability of Blockchains." *Proceedings of 1st ERCIM Blockchain Workshop 2018. European Society for Socially Embedded Technologies (EUSSET)*, 2018. https://doi.org/10.18420/blockchain2018_04.

Lansing, Jens, and Ali Sunyaev. "Trust in Cloud Computing: Conceptual Typology and Trust-Building Antecedents." *ACM SIGMIS Database* 47, no. 2 (2016): 58–96.

Lindman, Juho, Matti Rossi, and Virpi Kristiina Tuunainen. "Opportunities and Risks of Blockchain Technologies in Payments– A Research Agenda." *Proceedings of the 50th Hawaii International Conference on System Sciences,* Maui, HI, ScolarSpace, 2017, 1533–42.

Lindqvist, J. "New Challenges to Personal Data Processing Agreements: Is the GDPR Fit to Deal with Contract, Accountability and Liability in a World of the Internet of Things?." *International Journal of Law and Information Technology* 26, no. 1 (2018): 45–63.

Loebbecke, Claudia, Bernhard Thomas, and Thomas Ullrich. "Assessing Cloud Readiness at Continental AG." *MIS Quarterly Executive* 11, no. 1 (2012): 11–22.

Makhdoom, Imran, et al. "Blockchain's Adoption in IoT: The Challenges, and a Way Forward." *Journal of Network and Computer Applications* 125, no. 2019 (2019): 251–79.

Mantelero, Alessandro. "AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment." *Computer Law and Security Review* 34, no. 4 (2018): 754–72.

Mell, Peter, and Timothy Grance. "The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology," Gaithersburg, MD: Computer Security Division Information Technology Laboratory National Institute of Standards and Technology, 2011.

Miri, Mina, Farbod H. Foomany, and Nathanael Mohammed. "Complying With GDPR: An Agile Case Study." 2018. https://www.isaca.org/Journal/archives/2018/Volume-2/Pages/complying-with-gdpr.aspx?utm_referrer=.

Panetta, Kasey. "5 Trends Emerge in the Gartner Hype Cycle for Emerging Technologies, 2018 - Smarter With Gartner." *Smarter with Gartner*. 2018. https://www.gartner.com/smarterwithgartner/5-trends-emerge-in-gartner-hype-cycle-for-emerging-technologies-2018/.

———. "5 Trends Appear on the Gartner Hype Cycle for Emerging Technologies, 2019 - Smarter With Gartner." *Gartner*. 2019. https://www.gartner.com/smarterwithgartner/5-trends-appear-on-the-gartner-hype-cycle-for-emerging-technologies-2019/.

Papadopoulou, Panagiota, et al. "Investigating The Business Potential Of Internet Of Things." *MCIS 2017 Proceedings*, Genoa, Italy, Association for Information Systems, 2017.

Perera, Charith, et al. "Sensing as a Service Model for Smart Cities Supported by Internet of Things." *Transactions on Emerging Telecommunications Technologies* 25, no. 1 (2014): 81–93.

Pham, P. L. "The Applicability of the GDPR to the Internet of Things." *Journal of Data Protection & Privacy* 2, no. 3 (2019): 254–63.

Politou, Eugenia, et al. "Backups and the Right to Be Forgotten in the GDPR: An Uneasy Relationship." *Computer Law & Security Review* 34, no. 6 (2018): 1247–57.

Restrepo Amariles, David, Aurore Clément Troussel, and Rajaa El Hamdani. "Compliance Generation for Privacy Documents under GDPR: A Roadmap for Implementing Automation and Machine Learning." Workshop of Jurix 2019, Madrid, Spain, 2019.

Reyna, Ana, et al. "On Blockchain and Its Integration with IoT. Challenges and Opportunities." *Future Generation Computer Systems* 88 (2018): 173–90.

Russo, Barbara, et al. "Cloud Computing and the New EU General Data Protection Regulation." *IEEE Cloud Computing* 5, no. 6 (2018): 58–68.

Samaniego, Mayra, and Ralph Deters. "Blockchain as a Service for IoT." *Proceedings of the 2016 IEEE International Conference on Internet of Things (IThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 2016.

Satariano, Adam. "Google Is Fined $57 Million Under Europe's Data Privacy Law." *The New York Times*. 2019. https://www.nytimes.com/2019/01/21/technology/google-europe-gdpr-fine.html.

Shim, J. P., et al. "Internet of Things: Opportunities and Challenges to Business, Society, and IS Research." *Proceedings of the 38th International Conference on Information Systems*, Seoul, South Korea, Association for Information Systems, 2018.

Sousa, Weslei Gomes de, et al. "How and Where Is Artificial Intelligence in the Public Sector Going? A Literature Review and Research Agenda." *Government Information Quarterly* 36, no. 4 (2019): 1–14.

Stankovic, John A. "Research Directions for the Internet of Things." *IEEE Internet of Things Journal* 1, no. 1 (2014): 3–9.

Su, Ning, et al. "Shared Services Transformation: Conceptualization and Valuation from the Perspective of Real Options." *Decision Sciences* 40, no. 3 (2009): 381–402.

Swan, Melanie. *Blockchain: Blueprint for a New Economy*. 1st ed. Cambridge, UK: O'Reilly Media, 2015.

Tamburri, Damian A. "Design Principles for the General Data Protection Regulation (GDPR): A Formal Concept Analysis and Its Evaluation." *Information Systems* 91, no. 2020 (2020): 101469. https://doi.org/10.1016/j.is.2019.101469.

Tesfay, Welderufael B, et al. "I Read but Don't Agree: Privacy Policy Benchmarking Using Machine Learning and the EU GDPR." i, 2018. https://doi.org/10.1145/3184558.3186969.

Truong, Nguyen Binh, et al. "GDPR-Compliant Personal Data Management: A Blockchain-Based Solution." *IEEE Transaction on Information Forensics and Security* 2, no. 3 (2019): 208–12. http://arxiv.org/abs/1904.03038.

Underwood, Sarah. "Blockchain Beyond Bitcoin." *Communications of the ACM* 59, no. 11 (2016): 15–17.

van Geelkerken, F. W. J, and K. Konings. "Using Blockchain to Strengthen the Rights Granted through the GDPR." *International Youth Science Forum "Litteris Et Artibus,"* (2017): 458–61. http://ena.lp.edu.ua.

Vegh, Laura. "A Survey of Privacy and Security Issues for the Internet of Things in the GDPR Era." *Proceedings of the 2018 International Conference on Communications (COMM)*, Kansas City, MO, IEEE, 2018.

Venters, Will, and Edgar A. Whitley. "A Critical Review of Cloud Computing: Researching Desires and Realities." *Journal of Information Technology* 27, no. 3 (2012): 179–97.

Wachter, Sandra. "Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR." *Computer Law and Security Review* 34, no. 3 (2018a): 436–49.

———. "The GDPR and the Internet of Things: A Three-Step Transparency Model." *Law, Innovation and Technology* 10, no. 2 (2018b): 266–94.

Walsh, Clara, et al. "New Kid on the Block: A Strategic Archetypes Approach to Understanding the Blockchain." *Proceedings of the Thirty Seventh International Conference on Information Systems*, Dublin, Ireland, Association for Information Systems, 2016.

Wang, Yunfan, and Anuj Shah. "Supporting Data Portability in the Cloud Under the GDPR." 2018. https://alicloud-common.oss-ap-southeast-1.aliyuncs.com/Supporting_Data_Portability_in_the_Cloud_Under_the_GDPR.pdf.

Weber, Rolf H. "Socio-Ethical Values and Legal Rules on Automated Platforms: The Quest for a Symbiotic Relationship." *Computer Law and Security Review* 36 (2020, April): 105380.

Xu, C., K. Wang, and M. Guo. "Intelligent Resource Management in Blockchain-Based Cloud Datacenters." *IEEE Cloud Computing* 4, no. 6 (2017): 50–59.

Zhao, Yuan, and Bob Duncan. "Could Block Chain Technology Help Resolve the Cloud Forensic Problem?" *Proceedings of Cloud Computing*, Singapore, IARIA, 2018.