Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 218 (2023) 2480–2493

Procedia Computer Science

www.elsevier.com/locate/procedia

International Conference on Machine Learning and Data Engineering

Data protection governance framework: A silver bullet for blockchain-enabled applications

Karisma Karisma[a] Pardis Moslemzadeh Tehrani[b]

[a] University of Malaya, Malaysia
[b] Fellow Member of the Centre of Regulatory Studies, University of Malaya, Malaysia

Abstract

Blockchain technology is taking centre stage in major industries, ushering in a new era of decentralisation and digitalisation. While blockchain has garnered widespread traction in various sectors, there remain many technological, operational, societal, and legal challenges in deploying blockchain, mainly attributable to its sheer novelty. With ensuing ruminations about data protection concerns and given the real threats posed by the increasing usage of blockchain, scholars have examined these underlying challenges faced by blockchain users and regulators globally. Trust-building issues, such as data protection breaches, warrant our attention due to the negative consequences that may manifest and concretise in any measurable manner, triggering fragmentation of blockchain-based applications and socio-technical assemblages. This paper proposes eight data protection indicators (DPIs) to assess the maturity levels of countries in addressing data protection challenges in the blockchain landscape. The DPIs can contribute to developing institutional and governance frameworks to spur the global diffusion of hard and soft law instruments and establish broader safeguards of blockchain users' data.

Keywords: Blockchain technology; data protection; governance framework

1. Introduction

The advent of blockchain technology (hereinafter referred to as blockchain) is a prelude to technological development in the automation of systems. The synthesis of its characteristics (i.e., decentralization and digitalization) portray that blockchain can simplify, transform, and streamline business processes. These unique operational features can reshape a plethora of business sectors. Blockchain is regarded as an 'architecture of trust,' incorporating cryptographically verifiable systems, distributed network mechanisms, and incentive mechanisms within an open-source software, enabling a technical architecture to facilitate 'trustless trust' as it can generate consensus on the actual state of the ledger without the need to trust centralized or third-party intermediaries or central validation and verification mechanism [1]. Besides that, blockchain comprises a multitude of peers within a system of publicly

10.1016/j.procs.2023.01.223

verifiable proofs, obliterating the necessity of any individual to be identified as the sole trustee and therefore removing the need to place one's trust on a single individual [2]. It enables interaction, engagement, and coordination among blockchain participants who do not necessarily trust each other [3]. Hence, the potential of blockchain is multifaceted and engrained with the core element of trustlessness, deep-rooted in the endeavour to preserve the integrity of the ledger.

However, blockchain is figuratively a double-edged sword, revealing a dual nature. From a vantage point, blockchain has an edge in data privacy. It is applicable for privacy-preservation purposes as it provides transparency across multiple chains and prevents data modification with the embedded feature of immutability. Despite the positive depiction of privacy preservation, blockchain does not necessarily promote only sublime interactions within the network but may trigger major conflicts with data protection regulations. The recent emergence and measurable manifestation of blockchain scholarship have afforded a better appreciation of threats and conflicts of blockchain with data protection regulations. While trustlessness is at the core of blockchain, trust-building legislation from the outer periphery that advocate societal values, rights, and freedoms attempt to hinder cascading and catastrophic effects of privacy and security risks.

The advent of blockchain can induce informational, decisional, and transactional data privacy issues. These problems warrant our attention due to the negative consequences that can concretise in any measurable manner, leading to the fragmentation of blockchain-based applications. Therefore, a viable approach is required to avert or mitigate the potential risks and inherent conflicts. This article addresses how countries can overcome such challenges by developing adequate governance solutions, design choices, and business practices. In addressing the disparate problem logics, this article pays particular attention to privacy by design to address the related challenges in a context-aware manner by factoring in appropriate safeguards for developing robust data protection and privacy-friendly technology. Accompanying the discussion of the above, this paper develops data protection indicators (DPIs) that have a bearing on the legal readiness and maturity levels of countries in developing blockchain-enabled solutions. The proposed DPIs are germane to enable countries to assess the interactions, engagements, conflicts, and challenges between emerging blockchain applications and legal and regulatory data protection standards promptly and with sufficient reliability. Hence, the primary contribution of this article is to develop a methodological toolkit to assess the level of preparedness of countries in ensuring safe, effective, and resilient personal data processing in the blockchain paradigm. DPIs can facilitate the enactment of comprehensive policies and regulations to increase the level of legal readiness in the blockchain domain with diverse problem logics.

This paper is structured as follows. In Part 2, we analyze the realities of data privacy breaches in the blockchain landscape by exploring the following data protection principles, namely (i) data minimization, (ii) purpose limitation, (iii) the right to rectification, and (iv) the right to be forgotten. Part 2 also elucidates DPIs 1 to 4 to assess the legal readiness levels of countries in addressing multiple data protection challenges in the blockchain landscape. DPIs 1 to 4 explore the presence of (a) data protection frameworks that provide the necessary safeguards to mitigate the risks of data breaches, (b) quasi-legal instruments as meaningful and operationalizable tools, (c) specific and adequate delineation of data subjects' rights, and (d) technology-agnostic methodology in adopting such regulations. Part 3 sets out four pertinent bases, namely (a) consent, (b) performance of a contract, (c) legitimate interests, and (d) legal obligations for lawful data processing in the blockchain landscape. This paper exemplifies DPI 5 to assess the legal readiness levels of countries by determining whether data protection frameworks delineate specific legal bases for data processing. Part 4 explores the privacy by design (PBD) framework which offers some consolation towards placating challenges of data protection regulations in a blockchain landscape. This paper explores the scholarly contribution of PBD as a vanguard of blockchain development, manifesting as a novel legal strategy throughout the blockchain lifecycle. Part 4 propounds the importance of integrating and codifying PBD in data protection policies and legislation to promote broad usability in mitigating data protection risks considering the multidimensional conflicts of blockchain with the data protection paradigm. The paper delves into soft law governance of privacy by design by exploring soft law principles developed by scholars Cavoukian and Hoepmann, respectively. It then explores the inconsistency between blockchain immutability and PBD specifications and the lack of certainty as to who is a data controller in a blockchain environment. After providing a comprehensive elucidation on the regulatory indicators,

this paper provides an exhaustive conclusion on integrating data protection indicators within data protection regulations to develop harmonized policy responses and governance regimes in light of blockchain deployment.

2. Data Protection Governance Framework

The rich variegation of scholarly literature has considered the potential data protection breaches from the widespread application of blockchain. Blockchain designs are incongruous with data minimization principles as each full node on a blockchain ledger can replicate and store the exact copy of transactional data. In a public blockchain, the transactional data are not limited to the inspection of trading parties but all nodes on the blockchain system [4]. In addition, previous information recorded on a blockchain ledger is immutable, and therefore it is practically impossible to delete transactional data [5]. As each block connects to the previous block, deleting the transactional data on one block may impair the functionality of the entire blockchain system. Data protection regulations prohibit the processing of unduly broad statements. However, in a blockchain system, there are complexities in identifying data controllers to (a) determine the means and processing of personal data and (b) take appropriate technical and organizational measures in compliance with data protection regulations [6]. It is salient to determine whether all full nodes qualify as data controllers independently or whether to allocate responsibility to blockchain developers or platform providers. Furthermore, other technical impediments arise, such as the inability to rectify inaccurate or incomplete data, owing to the difficulty of coordinating and addressing various nodes on the blockchain network to perform such modifications on local copies [7]. Due to the bulk of nodes on a public blockchain network, compliance with the right to rectification proves impossible. In essence, timely regulatory engagement is salient to address peculiar data protection challenges. A wait-and-see approach, amounting to a lack of urgency and responsiveness, may threaten the stability dynamics of blockchain and proliferate data protection infringements. The lack of an earnest and effective dialogue may hinder regulators' and industry players' participatory and deliberative collaboration to resolve the legal and regulatory challenges that plague blockchain systems.

Most countries have embraced (or are moving towards) a comprehensive data protection governance framework. According to the United Nations Conference on Trade and Development, 137 out of 194 nations (71%) have implemented data protection and privacy legislation [8]. The remaining nations are either in the drafting stage of the legislative process or lack any legislative framework. Based on cross-country comparison, countries have embraced asymmetrical data protection laws. It is noteworthy that while many European Union Member States are frontrunners in extensive data protection legislations, other developed and developing countries strive to modernise their legal and regulatory frameworks to ensure adequate data protection. Several countries have adopted lenient approaches and lag in affording infallible data protection legislation. As regulatory engagement should be at the forefront of the global blockchain agenda, we elucidate the DPIs that can assess the legal readiness and maturity levels of countries considering data protection challenges.

- *DPI 1: The underlying question is whether the legal framework of a country addresses personal data protection.*

Personal data protection regulations play an indispensable role in fortifying blockchain-enabled solutions. A comprehensive data governance regime advances the right of informational self-determination and heightened control over the personal data of a data subject by codifying basic principles relevant to the processing of such data [9]. While the nuances of blockchain architecture and configuration raise the question of legal compliance, there is an ongoing dialogue concerning the harmonious interpretation of blockchain with data governance frameworks [10]. An ideal blockchain design is purposeful towards technical and organizational measures while ensuring compliance with data protection regulations and affording robust protection for the data subject. Through DPI 1, we assess the legal readiness and maturity levels of countries in adopting blockchain systems by the presence of overarching data protection frameworks and integration of necessary safeguards that would mitigate the risks of data breaches.

- *DPI 2: The subsequent question is whether specific guidelines and opinions on data protection have been issued by countries, and whether reference is made to blockchain.*

The lack of legal certitude in implementing compliant blockchain-enabled solutions may result in gaping pauses and impasses in developing blockchain. The assemblage of non-binding rules or instruments, namely regulatory guidelines, standards, and codes of conduct, can inevitably frame and inform our understanding of legally binding

data protection frameworks. Such non-binding texts provide practical and structured guidance to state and non-state actors towards ensuring compliance with data protection regulations, particularly with self-evident intricacies surrounding blockchain architectures [11]. Through DPI 2, we assess the legal readiness and maturity levels of countries adopting blockchain systems by implementing quasi-legal instruments as meaningful and operationalizable tools, both in general and specifically relating to blockchain.

- *DPI 3: An ensuing question is whether the data protection framework of a country adequately defines the rights of data subjects.*

Given the novelty of decentralisation and digitalisation, countries are obliged to ascertain the congruity of blockchain-enabled solutions in line with the rights and freedoms of data subjects enshrined in legal and regulatory frameworks. They adopt this position because any potential conflict or friction may conduce a drastic swing of the pendulum towards violation of such rights and freedoms. Therefore, it is pivotal to clearly define the scope of rights of the individual to data privacy, as broadly defined rights may fail in the intended protection of the individual. Through DPI 3, we assess the legal readiness and maturity levels of countries in adopting blockchain systems vis-à-vis the specific delineation of data subjects' rights.

- *DPI 4: In furtherance to the above (DP1 to DP3), whether the data protection framework of a country applies to public and private blockchain systems.*

The application of blockchain-enabled solutions can compromise the integrity of data. Therefore, in the absence of specific laws (or provisions) concerning the applicability of data protection regulations to public and private blockchain systems, countries are obliged to adopt a technology-agnostic methodology in interpreting such regulations. This position demonstrates that data protection regulations have a bearing on and are applied assiduously to blockchain systems. Through DPI 4, we explore the legal readiness and maturity levels of countries in adopting blockchain systems by considering the technologically neutral characteristics of data protection regulations.

3. Fortifying lawfulness of data processing activities

Prohibiting the processing of personal data in the absence of any lawful basis for such processing safeguards the rights of data subjects. Therefore, the following question is whether the data protection framework of a country delineates specific legal bases for data processing (DP 5). The General Data Protection Regulations of the European Union (GDPR) elucidates six bases for lawful processing, namely (a) consent, (b) contract, (c) legal obligations, (d) vital interests of data subjects, (e) public interests, and (f) legitimate interests. Discussion on the above has undergone rigorous academic and practical discourse. As such, the ensuing analysis appertains to the lawfulness of processing of personal data in the blockchain landscape, vis-à-vis criteria (a), (b), (c) and (f).

3.1 Consent

Consent is a valid and prominent feature of legal bases for data processing. The GDPR sets a high bar by requiring consent for data processing to be specific, informed, and freely given by the data subject with an unambiguous agreement vide a clear affirmative action, in line with the Notice and Choice framework. In one school of thought, scholars have contended that data subjects implicitly consent to process their personal data when creating a Bitcoin account or wallet [12]. However, scholars Read & Pehlivan oppose this postulation because the elements of 'affirmative action' and 'specificity' underlying the ambit of consent are not satisfied [13].

Scholars acknowledge the exiguity in maintaining meaningful data control while enhancing individual agency and autonomy of data subjects in blockchain systems, particularly attributable to their multifaceted and expansive paradigm. Personal data is in a perilous position due to power inequalities circumjacent to collecting and processing data between actors in light of emerging technologies. Hence, scholars and academics are largely agnostic about the efficacy of 'consent' as one of the more well-known legal bases for personal data processing [13]. While blockchain enforces a high level of transparency when performing data processing activities, which by and of itself yields informed consent, defining and specifying its purpose may be an arduous endeavour. In the latter instance, consent is reduced to a mere formality, consequential to the lack of specific purpose(s) of data processing in the blockchain landscape.

Each block connects to the preceding block via a cryptographic generic function in a blockchain network, and full nodes on the network retain a complete copy of the blockchain [14, 15]. In what follows, when contemplating participation in the blockchain network, the data subject is acquainted with and cognizant of processing one's personal data for the entire duration of the blockchain lifecycle [16]. While it is pivotal to preserve full functionality of the blockchain ledger by processing personal data until the end of the blockchain cycle, obtaining generic consent in lieu of specific consent from data subjects for such purpose does not achieve the quality of consent as codified in data protection regulations. In what follows, blockchain users cannot possibly circumvent or consent out of data protection provisions designed for their protection, such as the right to be forgotten. Consent is not a silver bullet in data processing activities, as data subjects can withdraw their consent at any time. In such circumstances, processing activities must cease, and data erasure occurs, the latter of which is challenging to comply with, due to the immutability feature of public blockchains. To circumvent the potential conflict between blockchain systems and the right to be forgotten, the author considers the privacy by design mechanism.

3.2 Performance of a contract

According to Article 6 of the GDPR, processing of personal data is lawful if it is "necessary for the performance of a contract to which the data subject is party" [17]. To rely on such a legal basis requires outlining the terms of the contract in advance and interpreting the legal provision strictly, in that processing the subject's data must be "genuinely necessary" for the performance of the contract. For instance, when a payment is made via digital tokens in the energy sector, the recipient's public address is utilized for energy transactions and made visible to the public blockchain network. In such a situation, the recipient cannot inveigh against such processing, as it is an integral part of the fulfilment of the supply contract [18]. On the other hand, a blockchain provider wishing to process data for marketing purposes cannot invoke contractual necessity as the basis of processing.

3.3 Legitimate interests

Another variant is pursuing the legitimate interest as a legal basis for data processing. This position materializes in situations where "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party," save the overriding of such interests by the fundamental rights and freedoms of the data subject [17]. The existence and application of this variant necessitate a careful assessment, considering reasonable expectations the data subject would have, "at the time and in the context of the collection of the personal data," in relation to the processing for that purpose [17]. It is highly doubtful that individuals participating in energy transactions would reasonably expect processing of their personal data (i.e., public keys) to materialize, beyond the energy transaction itself. Most blockchain users are unaware that (a) public keys on the blockchain network, having achieved a state of pseudonymization, are considered personal data; and (b) completed transactions recorded on the blockchain network divulge information about the data subject [11, 13]. When relying on the legitimate interest criterion as a legal basis for personal data processing, assessment of its use on a case-by-case basis involves the application of the necessity test, the balancing test, and the legitimacy test respectively; discussion of which are beyond the scope of this paper [19].

3.4 Legal obligations

Compliance with legal obligations is tantamount to another lawful basis for data processing. This position includes data controllers' obligations under anti-money laundering and combatting the financing of terrorism laws.

In summary, while we recognize the diversity and heterogeneity of data processing activities embarked on the blockchain network, determining the lawfulness of such activities remains an indispensable prerequisite to safeguarding the data protection rights of data subjects. Through DPI 5, we examine the legal readiness and maturity levels of countries in adopting blockchain systems, by considering the nature and scope of 'lawful bases for data processing activities' embedded within their legal and regulatory framework.

4. Privacy by Design framework – A boon to blockchain technology

An inadequate and ill-designed blockchain system may expose it to subtle (and apparent) technical and structural flaws because privacy is not the primary and foremost concern of technology developers, resulting in a myriad of

vulnerabilities which unwittingly forms within the system. Given the ongoing friction between blockchain and data protection regulations and the absence of a ready-made solution, theoretical and practical insights are necessary to address privacy by design frameworks, which may offer some consolation towards placating the blockchain data protection regulations predicament. Privacy by Design (PBD) is a concept that coalesces data protection principles with business practices, systems, and solutions, from the embryonic phase, through the entire lifecycle of the product [20]. Technology developers identify privacy threats at the outset during the initial experimental milieu vis-à-vis blockchain prototypes, living labs, and pilot projects to seamlessly embed suitable design specifications that address these threats into technological architectures on a case-by-case basis. Hence, regulators can traverse PBD principles toward a prospective path-dependent framework, contingent on technological development.

The potential of PBD in associating system designs with data privacy obligations within the blockchain arena remains largely unexplored. In the following section, the author elucidates the ensuing scholarly contribution of PBD in technological landscapes. According to Wirth & Kolain, it is intrinsically essential to pursue the concept of PBD when dealing with personal data, which is rudimentary to information technology systems [21]. In what follows, Wirth & Kolain attempt to translate legal prerequisites into technical guidelines and solutions as a manifestation of architectural blueprints, acknowledging the dearth of a comprehensive methodological tool in employing PBD within blockchain contexts [21]. Likewise, Chhetri implements a "regulation-to-code" design process that translates data protection regulations into objectives defined by the Standard Data Protection Model (SDPM) and reflects the perspicuous technical and organizational measures embedded within technological architectures by adopting a machine-readable data format [22]. Fabiano offers a starting point to address privacy and data protection concerns by alluding to the importance of PBD [23]. According to Cuquet & Fensel, PBD as a present-day accountability framework sets the stage for transparency and trust in protecting personal data [24]. Developing technical solutions disentangle such conflicts caused by the apparent friction between blockchain systems and data protection regulations. In what follows, by design, "data-oriented and "process-oriented" strategies are embedded into the blockchain architecture of the proposed system [5].

While PBD is one of many commonalities for resilient, secure, and privacy-aware systems and architectures from the ground up, its widespread implementation is achievable through the presence of a proper regulatory framework which recognizes the PBD concept [25].

4.1 Codifying privacy by design as a data privacy-enhancing feature

At this juncture, it is essential to embark on and develop data protection policies and legislations which accommodate a comprehensive and integrated privacy by design framework [26]. In such a situation, the law is considered as a tortoise, ploughing laboriously behind the technological hare, resulting in a regulatory gap, which PBD can partially bridge. What is required is a fundamental reorientation of data protection regulations in countries that have yet to recognise and implement PBD as a legally binding obligation. PBD is at the vanguard of blockchain development, manifesting a novel legal strategy and a viable tool with a highly effective framework. Scholars have acknowledged PBD as an imperative and indispensable prerequisite to attaining a high level of privacy and data protection when designing and developing technical systems, products, or services.[27] Many regulatory bodies are cognizant of its significance, including but not limited to the UK Information Commissioner's Office (ICO), Office of the Australian Information Commissioner, Information and Privacy Commissioner's Office, Canada, EU Article 29 Working Party, and the European Data Protection Supervisor. While in some countries, the development of the PBD framework is in the pipeline, in other countries invoking the legislative process is underway [28].

GDPR provisions enshrine modern risk-based approaches (i.e., PBD), embedded within devices and system architectures [29]. PBD introduced under Article 25 of the GDPR, elucidates that the controller must employ suitable technical and organisational measures to effectively implement data protection principles and safeguard the data subject's rights. To reckon with this proactive approach is to consider the state-of-the-art, cost of implementation, nature, scope, context, and purpose of processing, including the risks (of varying likelihood and intensity) posed by data processing towards individual rights and freedoms. In entrenching PBD principles, Recital 78 articulates an array of measures, including (a) minimising the processing of personal data, (b) adopting pseudonymisation techniques, and

(c) encapsulating transparency during data processing, among others [17]. Hence, a foundational step underlying PBD is engineering blockchain systems to minimise personal data processing via a multitude of pseudonymisation and anonymisation techniques [30].

The DPBD provisions codified under GDPR have precipitated similar national regulations in various countries, creating momentum for a holistic and beneficial transition in global data protection norms. The Federal Data Protection Act of Germany (BDSG) transposed the GDPR into national data protection law which came into effect on 25 May 2018. Like the GDPR, the BDSG of Germany emphasises the PBD requirements under Section 71 of the BDSG [31]. The adoption of PBD within the blockchain landscape is accentuated under the German Federal Blockchain Strategy by necessitating blockchain developers to embrace existing technical measures, PBD and PBDf respectively [32]. According to the Federal Government of Germany, the inevitable presence of blockchain does not necessitate the reorientation of GDPR. Instead, blockchain needs to be designed and utilised by data protection requirements. The ambivalence and uncertainty between blockchain developers and users of blockchain-enabled solutions ought to be attended to, so as to champion the development of blockchain that embraces the demands of data protection [32].

Switzerland recently incorporated the privacy by design provision into the Federal Act on Data Protection (FADP). The Federal Council Report has explicated the notion of PBD given blockchain development [33]. Compliance with data protection regulations can be established by designing and adopting appropriate technical and organisational measures to ensure transparency and bestow blockchain users more control over their personal information [34]. The Spanish Data Protection Authority (AEPD) recently published a guidance paper to facilitate blockchain development coherent with data protection legislation. The guidance paper recommends that blockchain developers review the PBD guide before adopting blockchain-enabled solutions [35]. In 2018, the French Data Protection Authority (CNIL) published a report regarding blockchain and GDPR, advocating PBD principles to safeguard data privacy and requiring data controllers identified by businesses to maintain constant vigilance against the data privacy and data integrity threats [36]. While there is a boisterous emphasis on data protection in Australia, there are no specific requirements concerning the implementation of PBD in legal and regulatory regimes. Nonetheless, the Office of the Australian Information Commissioner (OAIC) recommends the adoption of PBD as a measure of good practice. Some scholars have postulated the importance of proactive engagement considering technological developments by implementing PBD regimes that fortify trust and accountability in recent years [37].

Considering the challenges to societal values, it is pivotal to place primacy on the users' interest when developing a technology-driven framework. Blockchain users form the core substrate of the PBD model throughout the entire lifecycle of the system or product. Therefore, in developing design specifications for blockchain systems, developers must consider whether feasible measures are in place to safeguard the right to data privacy [23].

4.2 Embedding Privacy by Design into Data Protection Regulations

While scholars have framed the PBD to constitute a workable solution in the blockchain landscape, there is a dearth of an overt embodiment of PBD provisions in legal and regulatory frameworks. Laws must align with prevailing information technology infrastructures, such as blockchain systems, and for countries to prescribe a legal platform for incorporating a binding PBD framework, as a policy tool to develop technical and organisational measures and potentially limit risks of data privacy breaches. As a valuable provision, countries have underemphasised the importance of PBD and how it may be indispensable for agile technological development [38]. Therefore, PBD forms an essential indicator for the authors' proposed DPI framework. It mitigates data privacy risks arising from multi-dimensional conflicts of the blockchain-data protection paradigm. It is pivotal for data protection authorities to engage proactively and promote the inclusion of PBD mechanisms in legal and regulatory frameworks rather than adopt the wait-and-see approach.

DPI 6: The cardinal question is whether data protection legislation(s) of a country embraces a PBD framework.

DPI 7: In furtherance to DPI 6, whether the PBD framework of a country promotes broad usability in variegated contexts by (a) serving as a domain-agnostic instrument and (b) advances suitable technical and organizational measures in implementing data privacy principles effectively.

4.3 Soft-law governance of Privacy by Design

Statutory regimes are merely a means to an end and not an end itself. These regimes should complement the flexible and diverse embodiment of soft law instruments with implementable components integral for fast-emerging environments. Even if regulation of PBD is at the legislative level, the breadth of its application is contingent on multi-stakeholder governance processes in the blockchain landscape. This position is vis-à-vis non-binding soft-law instruments, such as principles, standards, guidelines, voluntary codes of conduct, and strategies [39]. In what follows, the extensive reliance on soft-law developed by state and non-state actors can suffuse our understanding of binding legal rules and obligations, facilitating practical actions and privacy-friendly technological designs and architecture.

DPI 8: The underlying question is whether specific principles, standards, guidelines, strategies, and codes of conduct concerning the PBD framework are advanced by countries.

In the following section, the author discusses globally verified key components of PBD developed by Ann Cavoukian. The seven pillars of PBD gleaned from the Fair Information Practices (FIP) principles inaugurated by Cavoukian take centre stage in defining the virtues of PBD, providing compelling reasons to address these pillars in-depth.

- Proactive not reactive.

PBD is an ex-ante proactive, forward-looking measure, rather than an ex-post reactive measure. Such a characterisation anchors on the anticipation of privacy-invasive events ahead of time [40]. As a prime solution, it facilitates a collective equipoise between functionality that is advantageous to blockchain development and safeguarding the rights and freedoms of blockchain users.

- Privacy as the default setting

The default blockchain configuration should be privacy-enhancing towards maintaining technological utility without requiring blockchain users to take adaptive and mitigative measures to protect their personal information [41]. Incorporating pivotal data privacy facets into blockchain systems during the engineering process allows the systems to remain intact throughout the blockchain lifecycle.

- Privacy embedded into design

Privacy is weaved into blockchain design and its architectural fabric holistically and comprehensively without a deconstructed and fragmented outlook. Based on this precept, separating the strands of data privacy from the core functionality of blockchain components, integrated and identified within the whole system, is impossible. An overarching narrative echoed across academic literature is that privacy is not an “add -on” but a constitutional component of blockchain.

- Full functionality – Positive sum, not zero sum

PBD seeks to employ a positive-sum approach by realizing legitimate interests and objectives. This position is attained vis-à-vis its contemporaneous existence and augmentation, as opposed to engaging in superfluous trade-offs that reflect the zero-sum dilemma in the blockchain landscape.

- End-to-end security-Lifecycle Protection

PBD accentuates the need for rigorous end-to-end security measures throughout the entire data lifecycle, from the phase of data collection until the deletion of the data. Executed in a timely fashion, it serves to avert security dilemmas that may materialize organically during the progression of the phase.

- Visibility and transparency

PBD ensures stakeholders that management of personal data vis-à-vis associated technology, systems, or business processes are compliant with the defined objectives. Any interested party can effectively verify such compliance, given that constituents of blockchain systems and operations are visible and transparent.

- Respect for user privacy

The interest of individuals is paramount. To that end, technology developers and operators ought to adopt mitigation-strategy measures that counter potential privacy breaches. Such measures must embrace (a) cogent privacy by default framework, (b) user-friendly options, and (c) appropriate privacy notices.

Interestingly, Dworkin, a leading philosopher, illustrates the pivotal role of widely held principles as a growing body of soft law which can steer the progressive and collective development and application of the law. Dworkin

considers principles as observable standards which are prerequisites for justice, fairness, or facets of morality [42]. The bedrock of sound PBD principles, such as that provided by Cavoukian, purport to guide conduct and provide a clear direction in realising legal goals and objectives delineated under data protection and privacy legislation. Even though principles are recognized as the "pacemaker of legalization", notable governance efforts are required to transpose foundational and exceedingly abstract principles (i.e., seven principles illustrated by Cavoukian) into implementable practical tools and regulatory guidelines.

That said, emphasizing a multitude of distinct legal strategies achieves specific policy outcomes. Innovation-proof and technology agnostic strategies can be developed to render PBD regimes efficacious, coherent, and resilient to ongoing blockchain development. Methodological approaches to devising strategies aligned with the abovementioned principles can enhance data integrity, confidentiality, visibility, and transparency of blockchain systems' design, operations, and management [43]. Therefore, in the same spirit as Cavoukian, Hoepmann articulates valuable privacy design strategies, categorised into "data-oriented strategies" and "process-oriented strategies", aiming to enhance privacy-preserving objectives, by translating legal requirements and principles into concrete design strategies. A brief overview is provided in Table 1 below. The novelty presented in this work lies in the fact that this paper proposes design strategies that can be implemented in the blockchain landscape in the form of guidelines. Guidelines that articulate operationalizable instructions can be utilised by blockchain developers for the optimal implementation of strategies [44].

Table 1. Privacy by design strategies in the blockchain landscape

Privacy by Design Strategies	Description	Guidelines in the implementation of design strategies in the blockchain landscape
	Data-oriented strategies	
Minimize **(Data collection phase)**	The amount of personal data to be collected is restricted to only what is relevant and necessary in achieving processing objectives. By minimizing the personal data collected, the privacy impact arising from any violation is reduced. This design strategy is aligned with the principle of data minimization and purpose limitation.	Storing personal data off-chain and embedding only the proof of existence of the information onto the ledger, such as the hash generated [45].
Hide **(Data collection, analysis, and storage phases)**	Personal data and its interrelationships must be kept hidden in a manner that prevents revelations, associations, legibility, and comprehensibility of such data, to avert any possible privacy violations. This strategy ensures confidentiality and incorporates the principle of data minimization.	• Data encryption and hashing schemes • Ring signature schemes can be utilized to hide transaction data and block headers (i.e., addresses) [46]. • Stealth address reduces linkability of users' addresses [47]. • Noise adding solutions for privacy-preserving performance of blockchain [48].
Separate **(Data storage phase)**	Personal data of the same individual derived from distinct sources should be processed and stored separately via distributed processing and storage, to make it more challenging to combine and correlate the data that can potentially divulge personal information. This design strategy achieves purpose limitation and provides adequate protection to data subjects.	Adopting a blockchain sharding scheme by splitting the files into different and smaller "shards" and storing the files on distinct nodes [49]. In situations where separation is not a viable option, notification can be provided via privacy policies

		and user agreements, and consent can be obtained.
Aggregate **(Data collection, analysis and use phases)**	The aggregate design strategy focuses on processing personal data at the highest level of aggregation with a limited amount of detail as far as it is possible to reduce privacy infringements. This design strategy incorporates principles of data minimization and purpose limitation.	• Ring signatures • Zero-knowledge proof is an effective tool to preserve data privacy and integrity as it proves the correctness of a statement without uncovering any information regarding the statement [50].
	Process-oriented strategies	
Inform **(Data collection phase)**	The product documentation, user agreement, and user policy should provide details on which information of the data subject is processed and the purpose and means of processing personal data. Data subjects should also be informed on third-party data sharing and data access rights. It ensures transparency and safeguards data subjects' rights.	Privacy policies and user agreements can be utilized.
Control **(Data collection phase)**	The control design strategy is a pivotal counterpart to the information strategy. It provides the data subject with the right to view, update, and request for deletion of the personal information of the data subject in a timely manner. The data subject can also decide whether to use a certain system for data processing pursuits and the type of information that is to be processed. This strategy reflects data portability and provides appropriate safeguards to data subjects' rights.	Storing data off-chain provides users with control over their data [49].
Enforce **(Data collection, analysis, storage, and use phases)**	A privacy policy incorporating legal requirements should be available to ensure commitment toward data protection. The privacy policy should be enforced by adopting appropriate technical measures and preventing data privacy infringements. This strategy reflects principles of purpose limitation, right to be forgotten, and data quality in achieving a specified purpose.	Privacy policies and user agreements can be utilized.
Demonstrate **(Data collection, analysis, storage, and use phases)**	This strategy ensures the availability of evidence to demonstrate compliance with privacy policy and data protection regulations.	Blockchain is a tamper proof and immutable ledger that provides an audit trail of all events [5].

Having considered the workings of various legal and regulatory modalities, the author postulates that hard law instruments are untenable and ineffective in the absence of soft law instruments. Therefore, state, and non-state actors should avail themselves of distinct regulatory instruments, such as principles, strategies, and guidelines in pursuing blockchain development.

4.4 Privacy by design at odds with blockchain architecture

i. Inconsistency between the immutability feature of blockchain and PBD specifications

Some scholars suggest the incongruity between PBD specifications with the features of blockchain, such as immutability, in that data is undeletable without breaking the chain [51]. While the concept of the right to be forgotten

occupies a central position in data protection regulations, excluding such a concept from the architectural blueprint of blockchain often occurs. It is evident that such exclusion serves to bolster the core component of blockchain (i.e., immutability), without which the application of blockchain is a moot point.

Nonetheless, in the recent years, scholars have put forward technical measures to address the inherent friction between the right to be forgotten and data protection regulations within the blockchain landscape, namely off-chain storage, pruning transactions on blockchain ledgers, encryption, chameleon hash, consensus-based voting, self-destruction, block matrix and private key. While these measures undoubtedly represent key data privacy-oriented approaches, their efficacy in ensuring compliance with data protection obligations is transitory and short-lived with emerging technical identifiers. For the nonce, developing a full-proof solution remains a chimaera of hope.

The author considers the assiduous diction of Article 25 of the GDPR as a source of solace and consolation given that it requires one to cogitate on state-of-the-art technology. It is not an isolated task considering its consonance with effective technical measures and control architectures presently available [52]. Hence, even if complete deletion appears to be paradoxical with the blockchain architecture, reliable and efficacious technical solutions prevalent in the blockchain landscape can constitute a suitable yardstick for privacy by design framework to ensure full compliance with data protection regulations [30].

ii. Upon whom does the obligation lie?

While PBD appears to be a clear and compelling solution surrounding the use of blockchain, the statutory obligation is not imposed directly on technological providers, platform integrators or developers, but on data controllers to ensure that appropriate data protection principles are employed to protect rights of data subjects and ensure full compliance with the requirements of the law [53]. At first glance, this appears to be counterproductive and inefficacious as controllers, in fulfilling their obligations, are required to instruct technology vendors to embed PBD measures into software and infrastructures. However, the proliferation of technology hampers the ability of developers to envisage the nature and extent of impact surrounding deployment.

In what follows, scholars and academics are undecided about who is considered a data controller, often vacillating between ‘nodes and miners’ or ‘blockchain users’ as data controllers. This area of contention has received significant attention in scholarly literature, in recent years.

Abdullah et al. presents 3 perspectives [5]. First, because nodes and miners (a) voluntarily engage in the blockchain network, (b) process personal data to maintain frictionless network operation, and (c) determine to a certain extent the means of processing such data, they tantamount to data controllers. Second, because nodes and miners have no control over the operation of blockchain systems and that of consensus mechanisms, they are not considered data controllers. Third, because blockchain users route their personal data into blockchain software for a predetermined data processing purpose, while being able to ascertain the manner and means of such processing they may be considered data controllers.

According to Read & Pehlivan, nodes that participate in the blockchain network, and facilitate the creation and validation of blocks in the ledger, may comprise of data controllers [13]. However, inevitably linked to this narrative is the difficult question on the application and enforcement of data protection regulations by anonymous nodes spanning across the blockchain network and proliferating in different jurisdictions [13]. As propounded by Tatar et al., while nodes preserve the full copy of the blockchain ledger, no node has absolute control over the entire network due to the unique characteristics of decentralization and digitalization that blockchain systems embody [51]. Thus, a more pressing question that remains unresolved is whether a node in the blockchain network is regarded as a data controller.

While it is important to elude a clear definition of data controllers in the blockchain landscape and broaden our understanding of the duties and responsibilities of such entities, the rights of data subjects can only be secured through appropriate operationalization mechanisms, especially in a decentralized environment. As academic discussions on

data controllers are still embryonic, Wirth & Kolain suggest the increased use of certification mechanisms that integrate with and complement PBD measures, and demonstrate compliance with data protection provisions [21].

5. Conclusion

In summary, considering the depth and breadth of its application, blockchain can trigger significant disruptive potential in numerous sectors. Even though the triumph of blockchain technology across industries has, by and large, eclipsed the focus on data transmission and protection, rigorous data protection principles engulf the authors' attempt to analyse and explore the realities of data protection infringements. When considering the legal and regulatory challenges associated with blockchain systems, perhaps we should be more modest in our claims, as blockchain issues remain unaddressed and inadequately regulated. The authors appraise the friction between data protection principles and blockchain architecture in this paper. The lack of integrated and comprehensive regulatory engagement may exacerbate data protection issues, generating perverse externalities in effectively deploying blockchain. As existing institutional and governance regimes of countries remain siloed and fragmented, it is essential to determine countries' legal readiness levels to address the data protection challenges and effectively implement working incentives to augment blockchain-based solutions. The authors develop DPIs to enable countries to assess their legal and regulatory engagements, frictions, and challenges between emerging blockchain applications and data protection principles promptly and with sufficient reliability. DPIs 1 to 4 assess countries' readiness levels by the presence of (a) overarching data protection frameworks, (b) hard and soft-law instruments, and (c) adequate definition of rights and freedoms of data subjects. Considering that the processing of personal data without legal bases should be prohibited, this paper has examined four critical legal bases for processing personal data in the blockchain landscape, which are indispensable as safeguards for data processing to protect the rights of data subjects.

In accompanying the discussions above, the authors exemplify the DPBD concept, which provides answers to the specific challenges posed in the blockchain landscape by emphasising common goals, societal values, and the rights and freedoms of data subjects during the initial stages of blockchain development vis-à-vis architectural configurations, designs, and patterns. This paper explores the salience of DPBD when handling personal data in the blockchain landscape, particularly as a novel strategy and a viable tool for effectively addressing data protection friction. DPIs 6 and 7 inquire whether data protection legislation advances a DPBD framework and serves as a domain-agnostic instrument to promote broad usability in the blockchain paradigm. This paper also considers the pertinence of soft-law instruments embodying DPBD provisions that encapsulate clear directions for achieving policy objectives and integrated governance regimes. Under DPI 8, the underlying question is on the trajectory of countries in advancing soft-law instruments that are congruent with the DPBD framework embedded into data protection regulations. The authors develop comprehensive assessment parameters, practical tools, and facilitating modalities in the form of DPIs to assess the readiness levels of countries. The DPIs shape the notion of regulatory models for blockchain-based solutions in a harmonised and coherent manner at macro and micro levels. By using the DPIs, regulators can draw meaningful insights on accountability and data integrity, paving the way for the overall operation of blockchain models. These precise and infallible indicators are readily achievable and equally implementable, as they identify the lowest common denominators in fostering blockchain innovation. Hence, countries can pass additional standards or legislation regulating blockchain-based applications and solutions by considering policy goals on the level of stringency or laxity. In essence, countries should converge towards an integrated and harmonised policy response by first appraising the latent conflicts and inadequacies in existing legal and regulatory frameworks and navigating the formation of institutional and governance regimes. Such a position would encourage blockchain users to participate fully and effectively in the blockchain fora.

Acknowledgements

The research for this publication is supported by a research grant from Quanta RegTech Capital PLC, International Funding of the University of Malaya under Grant Number IF057B-2018.

References

[1] Davidson, Sinclair, Primavera De Filippi, and Jason Potts. (2018) "Blockchains and the economic institutions of capitalism." *Journal of Institutional Economics* **14(4)**: 639-58.

[2] Swartz, Lana. (2017) "Blockchain dreams: Imagining techno-economic alternatives after Bitcoin", in Manuel Castells (ed). *Another economy is possible: Culture and economy in a time of crisis*.

[3] De Filippi, Primavera, and Samer Hassan. (2018) "Blockchain technology as a regulatory technology: From code is law to law is code." *First Monday* **21(12)**.

[4] Sim, Wie Liang, Hui Na Chua, and Mohammad Tahir. (2019) "Blockchain for identity management: The implications to personal data protection." *2019 IEEE Conference on Application, Information and Network Security (AINS)*: 30-5.

[5] Al-Abdullah, Muhammad, Izzat Alsmadi, Ruwaida AlAbdullah, and Bernie Farkas. (2020) "Designing privacy-friendly data repositories: a framework for a blockchain that follows the GDPR." *Digit Poli Regul Govern* **22(5-6)**: 389-411.

[6] Holzleitner, Marie-Theres, Katrin Burgstaller, Stephan Cejka, and Argjenta Veseli. (2020) "Electricity Trading via Blockchain in an Energy Community from a Data Protection Point of View." *European Energy & Climate Journal* **9(2)**: 33-43.

[7] Duarte, Diogo (2019) "An Introduction to Blockchain Technology From a Legal Perspective and Its Tensions With the GDPR." *Cyberlaw Journal of the Cyberlaw Research Centre of the University of Lisbon School of Law*.

[8] United Nations Conference on Trade and Development. "Data Protection and Privacy Legislation Worldwide" [cited 2022 April, 16]. Available from: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.

[9] Brotsis, Sotirios, Konstantinos Limniotis, Gueltoum Bendiab, Nicholas Kolokotronis, and Stavros Shiaeles. (2021) "On the suitability of blockchain platforms for IoT applications: Architectures, security, privacy, and performance." *Comput Networks* **191**: 108005.

[10] Shin, Don DH. (2019) "Blockchain: The emerging technology of digital trust." *Telematics and informatics* **45**: 101278.

[11] European Parliamentary Research Service Panel for the Future of Science and Technology. (2019) "Blockchain and the General Data Protection Regulation : Can distributed ledgers be squared with European data protection law?".

[12] Bacon, Jean, Johan David Michels, Christopher Millard, and Jatinder Singh. (2018) "Blockchain demystified: a technical and legal introduction to distributed and centralized ledgers." *Rich JL Tech* **25**: 1.

[13] Read, Inés Isidro, and Ceyhun Necati Pehlivan. (2020) "Blockchain and Data Protection: A Compatible Couple?" *Global Privacy Law Review* **1(1)**.

[14] Finck, Michèle (2018) "Blockchains and data protection in the European Union." *Eur Data Prot L Rev* **4**: 17-35.

[15] Panda, Sandeep Kumar, Siba Prasad Dash, and Ajay Kumar Jena. (2021) "Optimization of Block Query Response Using Evolutionary Algorithm", in *Data Engineering and Intelligent Computing*: Springer p. 573-9.

[16] Daoui, Sonia, Thomas Fleinert-Jensen, and Marc Lemperiere. (2019) "GDPR, Blockchain and the French Data Protection Authority: Many Answers but Some Remaining Questions." *Stan J Blockchain L & Pol'y* **2**: 1.

[17] General Data Protection Regulation, (2016).

[18] Article 29 Working Party. (2014) "Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC ".

[19] Janeček, Václav, and Gianclaudio Malgieri. (2020) "Commerce in Data and the Dynamically Limited Alienability Rule." *German Law Journal* **21(5)**: 924-43.

[20] Chik, Warren B. (2013) "The Singapore Personal Data Protection Act and an assessment of future trends in data privacy reform." *Computer Law & Security Review* **29(5)**: 554-75.

[21] Wirth, Christian, and Michael Kolain. (2018) "Privacy by blockchain design: a blockchain-enabled GDPR-compliant approach for handling personal data." *Proceedings of 1st ERCIM Blockchain Workshop 2018*.

[22] Chhetri, Tek Raj, Anelia Kurteva, Rance J DeLong, Rainer Hilscher, Kai Korte, and Anna Fensel. (2022) "Data Protection by Design Tool for Automated GDPR Compliance Verification Based on Semantically Modeled Informed Consent." *Sensors* **22(7)**: 2763.

[23] Fabiano, Nicola, (2017) "Internet of Things and blockchain: Legal issues and privacy. The challenge for a privacy standard." 2017 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): IEEE Published.

[24] Cuquet, Martí, and Anna Fensel. (2018) "The societal impact of big data: A research roadmap for Europe." *Technology in Society* **54**: 74-86.

[25] de Godoy, Jaqueline, Kathrin Otrel-Cass, and Kristian Høyer Toft. (2021) "Transformations of trust in society: A systematic review of how access to big data in energy systems challenges Scandinavian culture." *Energy and AI* **5**: 100079.

[26] Markatos, Evangelos (2022) "Policy Recommendations 2." *Cyber Security for Europe*: 38.

[27] de Terwangne, Cécile. (2021) "Council of Europe convention 108+: A modernised international treaty for the protection of personal data." *Computer Law & Security Review* **40**: 105497.

[28] Custers, Bart, Francien Dechesne, Alan M. Sears, Tommaso Tani, and Simone van der Hof. (2018) "A comparison of data protection legislation and policies across the EU." *Computer Law & Security Review* **34(2)**: 234-43.

[29] Amram, Denise. (2020) "Building up the "Accountable Ulysses" model. The impact of GDPR and national implementations, ethics, and health-data research: Comparative remarks." *Computer Law & Security Review* **37**: 105413.

[30] Jezova, Daniela. (2020) "Principle of Privacy by Design and Privacy by Default." *Regional L Rev*: 127.

[31] Federal Data Protection Act of 30 June 2017 (Federal Law Gazette I p. 2097), as last amended by Article 12 of the Act of 20 November 2019 (Federal Law Gazette I, p. 1626), (2017).

[32] Bundesministerium für Wirtschaft und Energie, and Bundesministerium der Finanzen. "Blockchain Strategy of the Federal Government" [Available from: https://www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/blockchain-strategy.pdf?__blob=publicationFile&v=3.

[33] Federal Act on Data Protection (FADP), (2019).

[34] Federal Council of Switzerland. (2018) "Legal framework for distributed ledger technology and blockchain in Switzerland: an overview with a focus on the financial sector." *Federal Council Report, available at: https://www newsd admin ch/newsd/message/attachments/55153 pdf (accessed 7th November, 2020)*.

[35] Agencia Española Protección Datos. "Blockchain (II): Basic concepts from data protection" 2020 [Available from: https://www.aepd.es/es/prensa-y-comunicacion/blog/blockchain-II-conceptos-basicos-proteccion-de-datos.
[36] French Data Protection Authority. Solutions for a responsible use of the blockchain in the context of personal data. 2018.
[37] Corbridge, Åste. (2018) "Responding to doxing in Australia: Towards a right to informational self-determination." *University of South Australia Law Review* **3**.
[38] Grünewald, Elias. (2021) "Cloud Native Privacy Engineering through DevPrivOps." *IFIP International Summer School on Privacy and Identity Management*.
[39] Demetzou, Katerina. (2019) "Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'high risk' in the General Data Protection Regulation." *Computer Law & Security Review* **35(6)**: 105342.
[40] Romanou, Anna. (2018) "The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise." *Computer Law & Security Review* **34(1)**: 99-110.
[41] Barbosa, Pedro, Andrey Brito, and Hyggo Almeida. (2020) "Privacy by Evidence: A Methodology to develop privacy-friendly software applications." *Inf Sci* **527**: 294-310.
[42] Dworkin, Ronald. (2013) "Taking rights seriously", A&C Black.
[43] Hoepman, Jaap-Henk, (2014) "Privacy design strategies." IFIP International Information Security Conference: Springer Published.
[44] Alkhariji, Lamya, Nada Alhirabi, Mansour Naser Alraja, Mahmoud Barhamgi, Omer Rana, and Charith Perera. (2021) "Synthesising privacy by design knowledge toward explainable internet of things application designing in healthcare." *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)* **17(2)**: 1-29.
[45] Mannan, Rosanna, Rahul Sethuram, and Lauryn Younge. (2019) "GDPR and Blockchain: A Compliance Approach." *Int'l J Data Protection Officer, Privacy Officer Privacy Couns* **3**: 7.
[46] Rahalkar, Chaitanya, and Anushka Virgaonkar. (2021) "Summarizing and Analyzing the Privacy-Preserving Techniques in Bitcoin and other Cryptocurrencies." *arXiv preprint arXiv:210907634*.
[47] Bergman, Karolina, and Saeed Rajput, (2021) "Revealing and Concealing Bitcoin Identities: A Survey of Techniques." Proceedings of the 3rd ACM International Symposium on Blockchain and Secure Critical Infrastructure; Published.
[48] Zhang, Xiaoyan, Shunrong Jiang, Yiliang Liu, Tao Jiang, and Yong Zhou. (2021) "Privacy-Preserving Scheme with Account-Mapping and Noise-Adding for Energy Trading Based on Consortium Blockchain." *IEEE Trans Netw Serv Manage*.
[49] Miyachi, Ken, and Tim K Mackey. (2021) "hOCBS: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design." *Information Processing Management* **58(3)**: 102535.
[50] Konkin, Anatoly, and Sergey Zapechnikov. (2021) "Privacy methods and zero-knowledge poof for corporate blockchain." *Procedia Computer Science* **190**: 471-8.
[51] Tatar, Unal., Yasir. Gokce, and Brian. Nussbaum. (2020) "Law versus technology: Blockchain, GDPR, and tough tradeoffs." *Comput Law Secur Rev* **38**.
[52] Grafenstein, Maximilian. (2020) "How to build data-driven innovation projects at large with data protection by design: A scientific-legal Data Protection Impact Assessment with respect to a hypothetical Smart City scenario in Berlin." *SSRN Journal*.
[53] Hildebrandt, Mireille, and Laura Tielemans. (2013) "Data protection by design and technology neutral law." *Computer Law & Security Review* **29(5)**: 509-21.