

Towards a Design Science Research Process for Legal Compliance by Design

Short Paper

Alexandra Hoess¹, Nadia Pocher¹, Tamara Roth^{1,2}, Gilbert Fridgen¹

¹Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg

²Sam M. Walton College of Business, University of Arkansas

{alexandra.hoess, nadia.pocher, gilbert.fridgen}@uni.lu, troth@walton.uark.edu

Abstract

The increasing complexity of IT-related laws and regulations pushes IS research to better integrate compliance into IS design processes. One key issue is the presence of often multiple legal provisions relevant to the same artifact. This generates tensions that can only be resolved through legal reasoning. Building on design science research and interdisciplinary literature, we explore features of a holistic design process based on legal reasoning to support legal compliance. We focus on the early stages of the design process - i.e., problem identification and definition of the objectives - and introduce two novel design activities: (1) analyzing the nature of requirements and (2) identifying and defining design trade-offs. Thereby, we develop a preliminary guideline to engage with legal experts. Our emerging method eases the transition into the design phase by putting legal reasoning before the definition of design objectives.

Keywords: Design science research, IS design, IT regulation, legal compliance by design

Introduction

Emerging digital technologies are increasingly ubiquitous, and pledge to deliver great benefits to society as a whole. Yet, their deployment and applications bring about challenges and risks that often call for legal safeguards. This directly concerns the information systems (IS) community, which focuses on bridging the technical aspects of IT and its business and social dimensions (Baskerville et al., 2018). Hence, IS researchers have been exploring how to integrate compliance with laws and regulations in their analyses and design of IS (Dickhaut et al., 2023b), the capabilities required for such integration (Labadie & Legner, 2023), and on how to leverage technology for legal purposes (Butler et al., 2023). This endeavor is of growing relevance due to the regulatory intensification in the digital sphere, with impacts that can transcend jurisdictional boundaries. An example is that of the EU General Data Protection Regulation (GDPR) (Weigl et al., 2023).

To establish design-based compliance and lower the associated costs, IS research has already explored how interdisciplinary knowledge can be codified and conveyed through patterns (Dickhaut et al., 2023a). When IT-related legal provisions become more complex and intertwined, however, their application becomes a matter of legal interpretation (Sartor, 2005). Typically, this requires the ability to address conflicts between requirements originating from different legal frameworks (Karasek-Wojciechowicz, 2021), but also among legal and other organizational or technical requirements that need to be reflected in the design of an IS. Such balancing exercise often results in trade-offs between applicable rules (Pocher & Veneris, 2022b).

Against this backdrop, compliance with laws and regulations needs to be considered holistically during IS design (Hoffmann et al., 2015). In this context, Design Science Research (DSR) provides a structured approach to reconcile prescriptive knowledge from different disciplines (Baskerville et al., 2018; Gregor & Hevner, 2013; vom Brocke et al., 2020). In particular, DSR's iterative approach of design and evaluation (Hevner et al., 2004; March & Smith, 1995) may help factor legal compliance into the artifact design early-on and avoid high costs of retrofitting it (Dickhaut et al., 2023b). Despite thorough research on designing (non-)functional requirements, so far, little guidance exists on what additional steps IS researchers and practitioners need to follow during the DSR process to holistically address compliance with laws and regulations in the design.

To adequately consider these dimensions, IS research would benefit from incorporating concepts of legal reasoning and a direct contact with legal experts into the design process. In this paper, we build on the interdisciplinary backgrounds of our author team, who stem from IS as well as IT law, to investigate: *How should the DSR process be refined to support legal compliance by design?*

To answer this research question, we build upon interdisciplinary research on design-based legal compliance and DSR, borrowing from critical approaches (Myers & Klein, 2011), and develop a preliminary method for holistic legal compliance – i.e., compliance with all relevant laws and regulations – by IS design. Our paper explores how DSR can guide collaborations between IS researchers, practitioners, and legal experts. By focusing on the early DSR phases, we consider an iterative four-step process for the validation of design objectives and trade-offs that will serve as input for design and development. We illustrate each of the four steps using the example of designing privacy-preserving central bank digital currency (CBDC) systems.

Theoretical Background

Design-based legal compliance in IS literature

In IS and related disciplines, literature has been exploring various manifestations of ‘designing’ compliance with laws and regulations for more than two decades. Existing IS publications on legal compatibility tried to integrate legal requirements through ‘compliance by design’. That is, they intended “to capture compliance requirements through a generic requirements modeling framework” (Sadiq et al., 2007, p.150) in an attempt to integrate legal requirements early on in the design. The goal of some related work is to achieve cost-effective independence from legal experts by providing developers with support to integrate legal requirements (Dickhaut et al., 2022). This can entail the codification of requirements into templates or ‘design patterns’ (Dickhaut et al., 2023b; Hoffmann et al., 2015). While design patterns provide relevant design knowledge, their application is often limited to a single legal field. In fact, accounting for multiple frameworks typically requires legal reasoning, which can benefit from legal automation only partially (Pagallo & Durante, 2016). In practice, legal reasoning can be difficult to abstract and codify into templates because of normative conflicts, for instance, that have different foundations. They can originate from the dynamics of the legal system, the co-existing protection of conflicting interests, or content uncertainties (Sartor, 1992).

Becker et al. (2014) make an initial attempt at a process-oriented approach to legal compliance in IS. Based on DSR, they propose a structured method that guides developers through the relevant steps to assess how legal requirements are reflected in the artifact and how changing laws and regulations will affect its compliance (and vice versa). A comparison between the intended design and implementation helps identify potential design-actualization-gaps. While this research provides an important milestone, Butler et al. (2023) emphasize the need for more research on how to reconcile IS design and relevant legal frameworks. This is because such reconciliation often requires risk assessments to resolve tensions among contending rules and requirements, which commonly depend on intensive socio-technical and legal reasoning of the proposed requirements, their actualization, and their implications.

To perform this reasoning, a nuanced understanding of the law is necessary. The reasoning already starts with determining if relevant frameworks are principle-based and/or rule-based (Braithwaite, 2002; Butler et al., 2023), which impacts the extent to which any balancing can be performed. All in all, little is known about how this type of reasoning can be integrated into the IS design process. Indeed, despite the efforts selectively outlined above, “the explicit consideration of legal compatibility in the development of applications is very rare” (Hoffmann et al., 2015, p.104), and IT regulation remains a “largely neglected area of IS” (Butler et al., 2023, p.86). Related research in the field of Law and Technology provides valuable perspectives on the need for legal compliance by design and its integration into the IS design process.

Design-based legal compliance in Law and Technology

In the past years, the relevance of ‘designing’ IT compliance has grown considerably in the research field termed Law & Technology, focused on regulating emerging technologies (Brožek et al., 2023). This was primarily driven by an increasing sensitivity to privacy and data protection vis-à-vis intensifying IT risks (Kanevskaia & Palka, 2023). At the same time, decentralization technologies and complex AI-based models

put to the test the capacity of traditional legal approaches to relate to, and constrain, these new ecosystems (Finck, 2018). At the origins of ‘compliance by design’, the often criticized ‘code is law’ paradigm highlighted the regulatory impact of code in the cyberspace (Lessig, 2006). It soon became clear that code does not replace law, but rather exerts a normative influence on individual behaviors together with market dynamics, law, and social norms (Filippi & Wright, 2018). Accordingly, code complements law in its regulatory action, and it is crucial to make a conscious decision about which values to embed (Finck, 2018). Over time, a new ‘law is code’ paradigm suggested law can be codified (i.e., defined as code) (Hassan & De Filippi, 2017), while smart contracts inspired governments to experiment with ‘rules as code’ (Casanovas et al., 2022).

Yet, the concept of reaching accountability (only) through code is commonly perceived in the Law & Technology field as an over-simplification with limited applicability. The regulatory action of code is useful only for objectively verifiable rules that can be defined in the code itself (Filippi & Wright, 2018). This applies to rules that are both unambiguous and easy to apply, which is not always the case. Above all, legal rules require semantic interpretation of the underlying meaning, grounded in legal reasoning (Pagallo & Durante, 2016). That is, code can never fully reflect human intentions, and semantic concepts are often too complex to be captured by binary computing logic. Bridging the two requires specific models (Athanasios et al., 2015). However, since “poorly designed code can be as harmful as poorly designed law” (Werbach, 2018, p.233), successful IT regulation requires a combined techno-legal focus (Pocher & Veneris, 2022b).

Parallel research streams have investigated the nature of legal requirements as compared to (non-)functional requirements in computer science and engineering (Casanovas et al., 2022). This question has been addressed also to support machine interpretation of and reasoning on legal content, and through various methodologies that range from goal-oriented requirements engineering, defeasible logic modelling, natural language processing, semantic annotation, legal ontology building, as well as legal compliance and validation processes (Palmirani et al., 2018; Soavi et al., 2002). Overall, the idea of streamlining compliance into a design process gained prominence through ‘privacy by design’ (Cavoukian, 2009). In later works, ‘(legal) compliance by/through design’ focused on embedding formalized rules but also legal interpretation into an artifact (Casanovas et al., 2017). This allows to consider context variables and the interpretation of legal rules, crucial to the design of legal compliance. It is also a flexible construct that accommodates the evolution of law, and shows how design-based compliance does not only refer to compliance with a text: when there are contending obligations, a compliance strategy also responds to a broader set of variables (Casanovas et al., 2022) – e.g., how to deal with conflicting requirements and tensions between legal principles.

Towards a DSR Method for Legal Compliance by Design

So far, little guidance exists on how DSR can accommodate for the evaluation of multiple legal principles and provisions. In this paper, we suggest a refined methodology focusing on the early stages of the DSR process, i.e., before the artifact is developed. Our starting point is the seminal work by Peffers et al. (2007) and their DSR methodology structured into six design activities: 1) *problem identification*, 2) *definition of design objectives*, 3) *design and development*, 4) *demonstration*, 5) *evaluation*, and 6) *communication*. While this method serves as a basis to develop prescriptive design knowledge, a step-wise approach may not account for the interconnection of complex problem spaces, where tensions between multiple legal fields, as well as technical and organizational requirements, encumber compliance (Rai, 2017).

In a development of this approach, Tuunanen et al. (2023) introduce design echelons, which constitute self-contained and interrelated activities of design and validation. These echelons have the capability to account for complex and interconnected contexts where “understanding the problem and formulating the research objectives [...] often requires several non-linear DSR iterations” (Tuunanen et al., 2023, p.2). This is of great relevance for legal compliance, where *problem identification* and *definition of design objectives* are often mutually constitutive and interdependent processes. Moreover, legal assessments are recursive processes that call for multiple iterations between the problem and solution spaces (Butler et al., 2023).

In particular, we note how legal reasoning often serves as a basis to identify if, how, and to which extent a requirement must be reflected in an artifact (Sartor, 2005). This is in strong relation with the nature of legal frameworks and provisions as principle-based and/or rule-based (Braithwaite, 2002). While in the first case there is typically more room for balancing conflicts, rule-based scenarios can manifest in the form

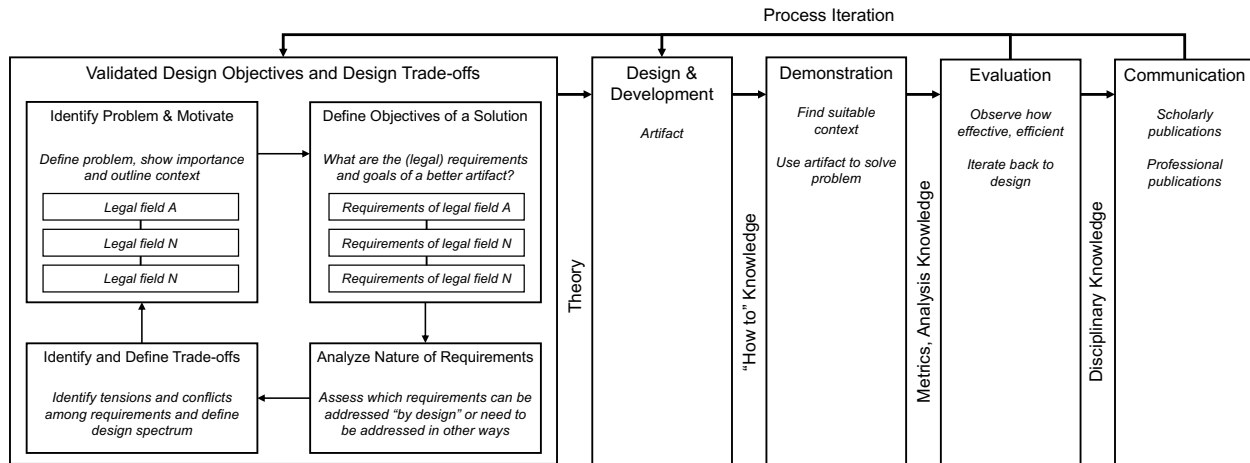


Figure 1. A DSR Method for Legal Compliance by Design – based on Peffers et al. (2007).

of an all-or-nothing application of a specific requirement. The latter case originates conflicts that are harder to balance by design. In hybrid cases composed of both principle-based and rule-based provisions (Butler et al., 2023), multiple requirements can be assessed in a context-specific fashion to determine precedence and resolution strategies as, for instance, data necessity and protection in the GDPR (Basin et al., 2018).

In our view, these characteristics call for two additional design activities focused on the *analysis of the nature of requirements* and *identification and definition of design trade-offs* to mediate iterations between the problem formulation and definition of design objectives. The resulting design trade-off expresses the resolution capacity in the form of a design spectrum (or continuum; (Tuunanen et al., 2023)). The four design activities combined can be viewed as one overarching design echelon that yields to *validated design objectives and design trade-offs*. The prescriptive knowledge about trade-offs and the validated design objectives serve as foundation for the subsequent design and development activity.

In the following, we describe this design echelon and each of its four design activities and their interplay, and provide a visual depiction of our preliminary method (Figure 1). For each activity, we provide a short example from CBDC systems, whose design is currently explored by more than 90% of central banks but so far typically yields publications focused on the designed product rather than on the design process (Hevner et al., 2004; Kosse & Mattei, 2023; Pocher & Veneris, 2022a).

Identify Problem and Motivate

In line with prior approaches, our preliminary DSR method starts with the fundamental activity of problem identification and formulation (Peffers et al., 2007; Sein et al., 2011). It outlines the relevance and properties of the problem space and previous solution approaches (vom Brocke et al., 2020). Establishing a rich problem formulation is crucial, as legal compliance often proves difficult and can only be achieved through a context-specific reflection (Butler et al., 2023). Corresponding analyses should focus on the underlying problem, relevant related theories, and help establish a rich understanding of the organizational context and, in particular, the legal fields in which the problem and its solution are situated.

IS research may therefore also benefit from design-oriented approaches that deeply engage with the artifact design in situ (Mullarkey & Hevner, 2019; Sein et al., 2011). Such broader reflection on the problem captures the distinct requirements of the institutional context of the artifact (Hashmi et al., 2018; vom Brocke et al., 2020). Interdisciplinary collaboration, especially the assistance of legal experts from different fields, can help contextualize the problem comprehensively and identify guiding (legal) frameworks that will inform, mandate, but also restrict, the features of a solution. In the case of a CBDC design that aims to address privacy-related problems (Choi et al., 2023), this could consist of identifying legal fields to be considered also beyond privacy and data protection – e.g., monetary law and the framework to prevent money laundering and the financing of terrorism (AML/CFT) (Pocher & Veneris, 2022a).

Define Objectives of a Solution

Informed by a first interdisciplinary formulation of the problem, IS research can transition to a more detailed analysis of the general objectives and the context-specific requirements of a better solution (Peppers et al., 2007; Tuunanen et al., 2023). This activity is not new to design-oriented research and valuable methodological guidance exists in various disciplines. IS research can therefore build upon existing methods to establish a more structured approach for this requirements analysis, such as requirements elicitation in requirements engineering (Hoffmann et al., 2015; Soavi et al., 2002). To ensure legal compliance by design, IS research can consult legal experts to analyze the requirements of each relevant legal field. In the case of CBDCs, this step could encompass the definition of the design objectives, such as ‘privacy’ and ‘accountability’ to comply with the AML/CFT regime. A more detailed requirements analysis would then focus on the identification of the principles and rules enshrined by, for instance, data protection and AML/CFT.

While identifying and analyzing the organizational, technical, and legal requirements of an improved artifact, IS research often uncovers conflicts between requirements and rules and/or tensions between principles. Such conflicts may develop from differences between dimensions (e.g., organizational, technical, and legal) or are the result of conflicting needs within one specific dimension. Prior research acknowledges the need for validating design objectives and requirements regarding their coherence, completeness, feasibility and operability (Tuunanen et al., 2023). We agree with the importance of such evaluation. Yet, we believe that coherence and avoidance of contradictions cannot always be (easily) achieved and requires additional guidance. Interdependencies and emerging conflicts should not distract throughout the initial collection of relevant legal rules. Instead, the focus should lie on gaining a holistic overview.

Analyze the Nature of Requirements

Either as part of the previous activity or as a subsequent step, IS researchers and practitioners should focus on a detailed assessment of the nature of each of the identified requirements. This is because there can be differences in the extent to which and how they can be designed into the emerging IS (Labadie & Legner, 2023). In other words, IS experts will have to identify which of the requirements can be addressed by design, through surrounding organizational processes, or call for a different way of implementation. In the case of CBDC design, the need for system ‘auditability’ can and must be considered during the design, but the extent of it (e.g., who can audit) needs to be set at governance level and balances the principles of privacy and transparency (see following step). Further, some requirements may need to be disregarded as they cannot be met, and in case of emerging technologies can often be discussed with regulatory and supervisory authorities to identify solutions (e.g., regulatory sandboxes, partial compliance (Casanovas et al., 2022)). In CBDC design, for instance, monetary law will need to be adapted to allow for their issuance, and the design activity cannot account for it per se (Pocher & Veneris, 2022a).

Concerning the nature of legal requirements, a detailed analysis should also investigate their origins. This may include whether they are rule and/or principle based and if these requirements are strict or can (in some cases also need to) be balanced against others (Sartor, 1992). Related assessments inevitably call for strong collaborations between legal experts and IS researchers and practitioners. While legal experts can provide assessments on the ‘legal’ nature of requirements and related leeway in their implementation, technical and organizational expertise is essential to identify if related technical implementations can be achieved and how these requirements should be treated in the actual development of the IS.

Identify and Balance Trade-offs to Address Conflicts among Requirements

Once a holistic overview of the design objectives and requirements as well as their nature has been achieved, IS researchers should turn to a more detailed analysis to identify and address emerging conflicts. The objective of this design activity is to identify and define trade-offs between different legal principles and rules and to analyze how and to what extent tensions and conflicts can be resolved. Thus, this design activity conceptually shifts the DSR process from the analysis of the problem space towards the concrete solution space that leads to synthesizing possible design requirements. As a starting point, IS researchers may illustrate design trade-offs by drawing spectra that enlist opposing requirements and principles at both ends. In the case of CBDC design, a frequent example relates to tensions between the need to safeguard privacy and data

protection, and mitigating the risk of illicit misuses. This typically manifests in the definition of a trade-off between privacy and transparency that needs to be considered in the design (Pocher & Veneris, 2022b).

The role of identifying trade-offs between principles and values in IS design has emerged strongly in literature. The designing process was described as a “process of trading-off, in which the pursuit of some design goals may directly counteract the achievement of others” (Wessel et al., 2024, p.2). We argue that the same applies in the legal domain. For each of the identified trade-offs, IS researchers may conduct an in-depth analysis of potential mitigation strategies (Sartor, 1992). Investigating how similar problems and conflicting requirements have been addressed in practice may provide valuable indications (vom Brocke et al., 2020). However, it is important to critically reflect on the projectability of preceding solutions, as in most cases, legal compliance cannot simply be copied or translated from one artifact to another. Related analysis will require legal reasoning to develop appropriate strategies for conflict resolution. For trade-offs arising from legal requirements, common approaches include a risk-based assessment to analyze the impact of meeting and neglecting the requirement(s) or the principle of proportionality (Gellert, 2017). Exhaustive reasoning will commonly require in-depth domain knowledge and the involvement of related experts (Sartor, 2005).

As such, this design activity will help IS researchers narrow down the design spectrum of the possible solution space, and produce prescriptive knowledge on design trade-offs and a corresponding validated set of design objectives and requirements. In many cases, the approach may not be the development of a unitary solution, but rather the investigation of so-called ‘design tiers’ to accommodate various trade-offs. In the design of CBDCs, one may address the privacy-transparency tension by integrating different trade-offs within the same system that selectively combine different design features for privacy and auditability based on a transaction’s risk. For example, privacy-enhancing technologies could be enabled for low-value transactions, but restricted for higher-value transactions (Michalopoulos et al., 2024; Pocher & Veneris, 2022b).

An Iterative Approach to Validated Design Knowledge

The reasoning illustrated above requires IS researchers to regularly revisit their initial problem statement and resulting definition of objectives, as of two reasons. First, many approaches to (legal) reasoning fundamentally build upon proportionality and impact assessment, which are naturally contingent on the underlying problem formulation. During this process, IS researchers may identify gaps in their problem formulation that need to be filled. Second, suggested trade-offs may also lead to restrictions of the solvable problem space – e.g., in the case of all-or-nothing requirements that cannot be balanced. IS researchers may therefore need to reconsider and gain a more detailed understanding of the problem. An updated problem formulation inevitably impacts the resulting objectives of a possible solution. Thus, IS researchers will have to refine identified objectives and requirements before proceeding to identify and define design trade-offs.

Such an iterative approach enables the gradual validation of the problem statement, objectives and requirements, as well as emerging design spectrum and trade-offs (Sonnenberg & vom Brocke, 2012). The validated knowledge will serve as input for the design and development and will be iteratively refined through recursive building and evaluation (Hevner et al., 2004; vom Brocke et al., 2020). It also acts as a research contribution itself (Baskerville et al., 2018; Tuunanen et al., 2023).

Expected contributions and future work

The plans for our future research comprise distinct but interrelated aspects. First, we plan to increase the level of detail in the description of our model. In particular, we aim to follow a holistic critical research approach (Myers & Klein, 2011) to further identify gaps in current DSR approaches and refine our preliminary method. By doing so, we particularly aim to focus on providing methodological guidance in the form of a process to conduct the balancing between contending legal rules and agree on a trade-off for a specific IT artifact. To this end, we will analyze in depth the variability among principles and requirements from various legal domains, as well as their interaction between other (non)functional requirements.

As a second stage of this research, we aim to expand our model to the subsequent steps of the DSR method, i.e., beyond those that precede the actual development of the artifact (Peppers et al., 2007). Specifically, we will tackle both the transition from validated design trade-offs to design and development (i.e., identification

of ways to concretely balance the requirements) and methodologies for the evaluation phase. We further aim to investigate how the design and development, demonstration and evaluation phases will feedback on the validated design trade-offs and how IS research can make best use of this feedback during the design iterations. This would allow us to derive design knowledge on where and how to approach interdisciplinary collaboration with domain and legal experts throughout the DSR process.

Third, we plan to address the pending need to evaluate and validate our preliminary DSR model, also by showing ways of concrete balancing between multiple legal principles and rules. To move in this direction, we plan to apply our emerging model to concrete cases related to digital identity and digital finance. We see prospects in the mentioned area of CBDCs, as the recent multi-stakeholder interest has generated a significant focus on the various policy and legal trade-offs to be designed and on the importance of interdisciplinary reasoning and cooperation (Kosse & Mattei, 2023). An example of a possible object of study is the spectrum between privacy and transparency that includes the tension between privacy, data protection, and financial integrity (Pochoer & Veneris, 2022b). Various reports exist that provide central banks with frameworks to take informed decisions regarding legal and policy trade-offs to be embedded into CBDC designs. To benefit from such empirical insights, we also aim to conduct a structured literature review and a comparative analysis of our method against academic and practitioner studies that report on the design of legally compliant IS in different real-world applications. Additional future research that explores the feasibility of our suggested DSR method in different contexts would also be important to assess and enhance its generalizability.

Lastly, while developing our preliminary DSR method for legal compliance through IS design, we experienced tensions between the need for context-specific solutions to achieve legal compliance and the generalizability of knowledge. In more detail, legal compliance typically approaches problems at the context-specific instantiation level, yielding contributions in the form of “situated implementations” (Gregor & Hevner, 2013). In turn, DSR, also strives for producing theoretical design knowledge that is applicable within a larger class of problems. Valuable future research could explore and evaluate whether and how our DSR method can be applied to produce generalizable and mature knowledge, such as “design principles” or “well-developed design theories” that are projectable to a class of problems (Gregor & Hevner, 2013).

Conclusions

In this paper, we introduced a preliminary DSR method for legal compliance by IS design. We focused on the early stages of the design process (i.e., the phases before the actual development of the artifact), as compliance with laws and regulations particularly hinges upon the problem and its context. We suggested additional design activities focused on analyzing the nature of requirements and the identification and definition of design trade-offs, which mediate iterations between the problem formulation and the definition of design objectives. Altogether, these four design activities can be viewed as one overarching design echelon that yields to validated design objectives and trade-offs. We emphasized the importance of collaboration with legal experts in the design process to analyze and weigh the requirements, before transposition into IS design. In our view, accommodating for interdisciplinarity in the early design stages supports the creation of artifacts with high technical feasibility and legal compliance.

Acknowledgements

This research was funded by the Luxembourg National Research Fund (FNR) and PayPal, PEARL grant ref. 13342933/Gilbert Fridgen, as well as grant ref. NCER22/IS/16570468/NCER-FT (CryptoReg). Supported by Banque et Caisse d'Épargne de l'État (Spuerkeess) and Luxembourg's Ministry for Digitalisation. For the purpose of open access, and in fulfillment of the obligations arising from the grant agreements, the authors have applied a CC BY 4.0 license to any Author Accepted Manuscript version arising from this submission.

References

Athan, T., Governatori, G., Palmirani, M., Paschke, A., & Wyner, A. (2015). Legalruleml: Design principles and foundations. In W. Faber & A. Paschke (Eds.), *Reasoning web* (pp. 151–188). Springer International Publishing. https://doi.org/10.1007/978-3-319-21768-0_6

- Basin, D., Debois, S., & Hildebrandt, T. (2018). On purpose and by necessity: Compliance under the gdpr. In S. Meiklejohn & K. Sako (Eds.), *Financial cryptography and data security*. Springer. https://doi.org/10.1007/978-3-662-58387-6_2
- Baskerville, R., Baiyere, A., Gregor, S., Hevner, A., & Rossi, M. (2018). Design science research contributions: Finding a balance between artifact and theory. *Journal of the Association for Information Systems*, 19(5), 3. <https://doi.org/10.17705/1jais.00495>
- Becker, J., Heddier, M., Bräuer, S., & Knackstedt, R. (2014). Integrating regulatory requirements into information systems design and implementation. *35th International Conference on Information Systems*.
- Braithwaite, J. (2002). Rules and principles: A theory of legal certainty. *Australian Journal of Legal Philosophy*, 27. <https://doi.org/10.2139/ssrn.329400>
- Brožek, B., Kanevskaia, O., & Pałka, P. (2023). *Research handbook on law and technology*. Edward Elgar.
- Butler, T., Gozman, D., & Lyytinen, K. (2023). The regulation of and through information technology: Towards a conceptual ontology for is research. *Journal of Information Technology*, 38(2), 86–107. <https://doi.org/10.1177/02683962231181147>
- Casanovas, P., De Koker, L., & Hashmi, M. (2022). Law, Socio-Legal Governance, the Internet of Things, and Industry 4.0: A Middle-Out/Inside-Out Approach. *J*, 5(1), 64–91. <https://doi.org/10.3390/j5010005>
- Casanovas, P., González-Conejero, J., & de Koker, L. (2017). Legal compliance by design (lcbd) and through design (lctd): Preliminary survey. *30th International Conference on Legal Knowledge and Information Systems (JURIX), Workshop on Technologies for Regulatory Compliance*.
- Cavoukian, A. (2009). *Privacy by design*. Information; Privacy Commissioner of Ontario, Canada.
- Choi, S., Kim, B., Kim, Y.-S., & Kwon, O. (2023). Central bank digital currency and privacy: A randomized survey experiment. Bank for International Settlements.
- Dickhaut, E., Janson, A., Hevner, A. R., & Leimeister, J. M. (2023a). Sharing Design Knowledge Through Codification in Interdisciplinary DSR Collaborations. *56th Hawaii International Conference on System Sciences*. <https://doi.org/10.24251/HICSS.2023.629>
- Dickhaut, E., Janson, A., Söllner, M., & Leimeister, J. M. (2023b). Lawfulness by design – development and evaluation of lawful design patterns to consider legal requirements. *European Journal of Information Systems*, 1–28. <https://doi.org/10.1080/0960085X.2023.2174050>
- Dickhaut, E., Li, M. M., Janson, A., & Leimeister, J. M. (2022). The role of design patterns in the development and legal assessment of lawful technologies. *Electronic Markets*, 32(4), 2311–2331. <https://doi.org/10.1007/s12525-022-00597-1>
- Filippi, P. D., & Wright, A. (2018). *The rule of code*. Harvard University Press.
- Finck, M. (2018). *Blockchain regulation and governance in europe*. Cambridge University Press.
- Gellert, R. (2017). We have always managed risks in data protection law: Understanding the similarities and differences between the rights-based and the risk-based approaches to data protection. *European Data Protection Law Review*, 4, 481–492. <https://doi.org/10.21552/EDPL/2016/4/7>
- Gregor, S., & Hevner, A. R. (2013). Positioning and presenting design science research for maximum impact. *MIS Quarterly*, 337–355. <https://doi.org/10.25300/MISQ/2013/37.2.01>
- Hashmi, M., Casanovas, P., & de Koker, L. (2018). Legal compliance through design: Preliminary results of a literature survey. *31st International Conference on Legal Knowledge and Information Systems (JURIX), Workshop on Technologies for Regulatory Compliance*.
- Hassan, S., & De Filippi, P. (2017). The expansion of algorithmic governance: From code is law to law is code. *Field Actions Science Reports*.
- Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, 28(1), 75–105. <https://doi.org/10.2307/25148625>
- Hoffmann, A., Schulz, T., Zirfas, J., Hoffmann, H., Roßnagel, A., & Leimeister, J. M. (2015). Legal Compatibility as a Characteristic of Sociotechnical Systems: Goals and Standardized Requirements. *Business & Information Systems Engineering*, 57(2), 103–113. <https://doi.org/10.1007/s12599-015-0373-5>
- Kanevskaia, O., & Pałka, P. (2023). Introduction to the research handbook. In B. Brožek, O. Kanevskaia, & P. Pałka (Eds.), *Research handbook on law and technology*. Edward Elgar.
- Karasek-Wojciechowicz, I. (2021). Reconciliation of anti-money laundering instruments and European data protection requirements in permissionless blockchain spaces. *Journal of Cybersecurity*, 1–28. <https://doi.org/10.1093/cybsec/tyab004>

- Kosse, A., & Mattei, I. (2023). *Making headway. results of the 2022 BIS survey on central bank digital currencies and crypto*. Bank for International Settlements.
- Labadie, C., & Legner, C. (2023). Building data management capabilities to address data protection regulations: Learnings from eu-gdpr. *Journal of Information Technology*, 38(1), 16–44. <https://doi.org/10.1177/02683962221141456>
- Lessig, L. (2006). *Code v. 2.0*. Basic Books.
- March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. *Decision Support Systems*, 15(4), 251–266. [https://doi.org/10.1016/0167-9236\(94\)00041-2](https://doi.org/10.1016/0167-9236(94)00041-2)
- Michalopoulos, P., Olowookere, O., Pocher, N., Sedlmeir, J., Veneris, A., & Puri, P. (2024). Compliance design options for offline cbdc: Balancing privacy and aml/cft. *2024 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. <https://doi.org/10.2139/ssrn.4770513>
- Mullarkey, M. T., & Hevner, A. R. (2019). An elaborated action design research process model. *European Journal of Information Systems*, 28(1), 6–20. <https://doi.org/10.1080/0960085X.2018.1451811>
- Myers, M. D., & Klein, H. K. (2011). A set of principles for conducting critical research in information systems. *MIS Quarterly*, 35(1), 17–36. <https://doi.org/10.2307/23043487>
- Pagallo, U., & Durante, M. (2016). The pros and cons of legal automation and its governance. *European Journal of Risk Regulation*, 7, 323–334. <https://doi.org/10.1017/S1867299X00005742>
- Palmirani, M., Martoni, M., Rossi, A., Bartolini, C., & Robaldo, L. (2018). Legal ontology for modelling gdpr concepts and norms. In *Frontiers in artificial intelligence and applications, volume 313: Legal knowledge and information systems*. <https://doi.org/10.3233/978-1-61499-935-5-91>
- Peffer, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*, 24(3). <https://doi.org/10.2753/MIS0742-1222240302>
- Pocher, N., & Veneris, A. (2022a). Central bank digital currencies. In *Handbook on blockchain*. Springer. https://doi.org/10.1007/978-3-031-07535-3_15
- Pocher, N., & Veneris, A. (2022b). Privacy and transparency in CBDCs: A regulation-by-design AML/CFT scheme. *IEEE Transactions on Network and Service Management*, 19(2), 1776–1788. <https://doi.org/10.1109/TNSM.2021.3136984>
- Rai, A. (2017). Editor's comments: Diversity of design science research. *MIS quarterly*, 41(1), iii–xviii.
- Sadiq, S., Governatori, G., & Namiri, K. (2007). Modeling control objectives for business process compliance. In G. Alonso, P. Dadam, & M. Rosemann (Eds.), *Business process management*. Springer. https://doi.org/10.1007/978-3-540-75183-0_12
- Sartor, G. (1992). Normative conflicts in legal reasoning. *Artificial Intelligence and Law*, 1, 209–235. <https://doi.org/10.1007/BF00114921>
- Sartor, G. (2005). Legal reasoning. *A Treatise of Legal Philosophy and General Jurisprudence*, 5.
- Sein, M. K., Henfridsson, O., Purao, S., Rossi, M., & Lindgren, R. (2011). Action design research. *MIS Quarterly*, 35(1), 37–56. <https://doi.org/10.2307/23043488>
- Soavi, M., Zeni, N., Mylopoulos, J., & Mich, L. (2002). From legal contracts to formal specifications: A systematic literature review. *SN Computer Science*, 3. <https://doi.org/10.1007/s42979-022-01228-4>
- Sonnenberg, C., & vom Brocke, J. (2012). Evaluations in the science of the artificial—reconsidering the build-evaluate pattern in design science research. *Design Science Research in Information Systems. 7th International Conference 2012*. https://doi.org/10.1007/978-3-642-29863-9_28
- Tuunanen, T., Winter, R., & vom Brocke, J. (2023). Dealing with Complexity in Design Science Research - A Methodology Using Design Echelons. *MIS Quarterly*.
- vom Brocke, J., Winter, R., Hevner, A., & Maedche, A. (2020). Special issue editorial—accumulation and evolution of design knowledge in design science research: A journey through time and space. *Journal of the Association for Information Systems*, 21(3), 9. <https://doi.org/10.17705/1jais.00611>
- Weigl, L., Barbereau, T., Sedlmeir, J., & Zavolokina, L. (2023). Mediating the tension between data sharing and privacy: The case of dma and gdpr. *31st European Conference on Information Systems*.
- Werbach, K. (2018). *The blockchain and the new architecture of trust*. MIT Press.
- Wessel, L., Sundermeier, J., Rothe, H., Hanke, S., Baiyere, A., Rappert, F., & Gersch, M. (2024). Designing as trading-off: A practice-based view on smart service systems. *European Journal of Information Systems*, 0(0), 1–26. <https://doi.org/10.1080/0960085X.2024.2308541>