Vol.4, Issue.3, (2025)
Journal of Advances in Humanities Research
https://doi.org/10.56868/jadhur.v4i3.321

Negligence and Data Breaches Under Saudi Arabian Personal Data Protection Law (PDPL): A Doctrinal Analysis Approach

Hanan Alnasser

Faculty of Law Universiti Malaya, Kuala Lumpur, 50603, Malaysia

Article Information

Article Type: Research Article

Dates:
Received: August 20, 2025
Revised: September 15,2025
Accepted: September19, 2025
Available online: September 20, 2025

Corresponding Author:
Hanan Alnasser

hananalnasser97@gmail.com

ABSTRACT

This study critically investigates the treatment of negligence under the Saudi Arabian Personal Data Protection Law (PDPL), aiming to diagnose its doctrinal weaknesses and propose evidence-based reforms. Employing a qualitative doctrinal legal research methodology to systematically investigate the treatment of negligence within the Saudi Arabian Personal Data Protection Law (PDPL). The analysis reveals the PDPL's core deficiencies: a critically vague standard of care, an enforcement gap lacking robust deterrents, and procedural lacunae in breach notification and accountability. The findings demonstrate that the law's undefined "appropriate measures" and reliance on a narrow deterrent model fail to effectively prevent or redress negligence-related data breaches. The study's primary implication is the proposal of a unique hybrid reform path, strategically synthesizing the GDPR's proactive accountability with the CCPA's private litigation model. A key novelty of this research is its grounding of these reforms within the culturally resonant principles of Islamic jurisprudence (أمانة Amanah, ضرر Ḍarar), reframing data protection not as a foreign import but as a modern extension of the Kingdom's ethical heritage, thereby offering a coherent framework for legislative strengthening and enhanced compliance.

Keywords: PDPL, Data Breach, Negligence, Data Protection Law, Islamic Jurisprudence, Regulatory Enforcement.

1. INTRODUCTION

The dawn of the 21st century has been defined by the rise of a global, data-driven economy (Hoofnagle et al, 2019). Personal information is now often referred to as the "new oil" (Nusairat, 2024). This transformation has fueled unprecedented innovation and economic growth, yet it has also triggered a widespread and escalating crisis globally (Kanojia, 2023). Organizations are accumulating vast amounts of personal information, making them highly attractive targets for malicious actors. This leaves an individual's vulnerable to financial exploitation, identity loss, reputation harm, and psychological anguish (Aldubayyan, 2023). In response, a patchwork of data protection laws has emerged at the international level. These laws aim to impose order on the digital frontier and to restore the balance of power between data subjects and controllers (Abdullah, 2020). Among these regulations, the General Data Protection Regulation (GDPR) of the European Union and the California Consumer Privacy Act (CCPA) stand out as robust frameworks for data privacy, security, and responsibility (Alzahrani, 2024). The GDPR relies on a core principle of data protection, emphasizing privacy by design, clear breach notification, and administrative penalties (Elgujja, 2020). The CCPA, developed as a consumer

protection law, enables individuals to manage their data and seek redress, particularly in breaches caused by inadequate security (Sarabdeen & Moonesar, 2018).

In this international context, the Kingdom of Saudi Arabia has implemented the Personal Data Protection Law (PDPL) as part of its Vision 2030 strategy (Alfaifi, 2024). The PDPL represents a historical move to align national legal standards with international expectations for the digital economy (Al-Saggaf & Weckert, 2011). The law outlines principles for the processing of personal data, grants rights to data subjects, and establishes a supervisory authority. As with any new law, its effectiveness in addressing the complex reality of data security breaches remains to be seen (Al Nafea & Almaiah, 2021). A significant gap in current academic and practical debates is how the PDPL addresses organizational negligence. While the law includes broad requirements for confidentiality and security, it does not clearly define negligent breaches or the standard of care required. The concepts of causation and harm also need adaptation for digital injuries (Abanumy et al., 2005).

A key issue in the Saudi PDPL is legal uncertainty from the lack of a specific negligence standard (Alharbi et al., 2021). Without a clear duty of care, organizations may be uncertain about whether their data protection practices are legally sufficient. Conversely, harmed data subjects may have no remedy if the harm stems from a lack of reasonable care (Al-Mashaqbeh, 2025).

Traditionally, the legal definition of negligence has bridged the gap between poor organizational practices and resulting harm. It has formed the basis for regulatory enforcement and civil liability (Alzahrani, 2024). This uncertainty in the PDPL hinders compliance for regulated parties, influences the enforcement priorities of the Saudi Data and AI Authority (SDAIA), and presents challenges for the judiciary (Alhashim & Rahman, 2021).

This research uses doctrinal analysis to study the PDPL and systematically analyzes its main text. It also applies a comparative analysis with the GDPR and CCPA to identify best practices and regulatory models. The analysis draws on multiple theories: Tort Law and Negligence Theory (Hoofnagle et al., 2019), Privacy Theories—such as autonomy and structural power (Westin, 1967; Zuboff, 2019), Organization Accountability Theory (Bygrave, 2017), and Islamic Jurisprudence concepts like ضرر-ḍarar (harm) and تقصير-taqšir (fault) (Corrales et al., 2021). This doctrinal approach allows for a critical examination of negligence under the Saudi PDPL. The research aims are:

1. To identify and critically analyse the implicit standards of care and liability for negligent data breaches within the PDPL's legal text and implementing regulations.
2. To evaluate the deterrent effect of the PDPL's current penalty regime against negligent data breaches by comparing the incentives for compliance it creates against the costs of non-compliance.
3. To conduct a comparative legal analysis of the frameworks for negligence, external data transfer, and breach notification under the PDPL, the EU's GDPR, and the California Consumer Privacy Act (CCPA), identifying key divergences and their practical implications.
4. To propose evidence-based recommendations for legislative and regulatory refinement of the PDPL, focusing on incorporating a clear, actionable standard of care to more effectively prevent and redress negligence-related data breaches.

To guide this analysis, the study will address the following research questions

1. How does the Saudi PDPL currently define, or implicitly address, the legal concept of negligence in the context of data breach liability, and what are the resultant legal uncertainties?

2. To what extent do the administrative fines and corrective measures under the PDPL provide an effective and proportionate deterrent against organizational negligence in data security practices?
3. What are the principal differences in how the PDPL, GDPR, and CCPA conceptualize a data controller's duty of care, regulate international data transfers, and mandate breach notification, particularly in scenarios involving a lack of intent?
4. Based on the findings, what specific amendments to the PDPL's provisions, or its implementing regulations, would most effectively establish a coherent standard of care and improve mechanisms for redress in cases of negligent data breaches?

This research fills an identified gap in the literature by focusing on the underdeveloped concept of negligence within the PDPL. While earlier studies have outlined the law's general provisions, there is a lack of in-depth doctrinal and comparative analysis concerning this specific liability standard. The novelty of this study lies in its targeted analysis of how the absence of a clear 'duty of care' undermines both the law's operational effectiveness and its alignment with global standards, leading to concrete legal recommendations to bridge this critical gap.

2. LITERATURE REVIEW

2.1 The Doctrinal Challenges of Negligence in Data Protection

Translating the concept of negligence from the traditional to the digital sphere is conceptually challenging (Drechsler & Kamara, 2021). Physical injuries are clearer, but data breaches often result in non-physical, statistical, and diffuse damages, making it difficult to prove proximate cause and injury (Kilovaty, 2021). In classic torts, a single event typically causes harm, but a data breach is a systemic breakdown. Thousands may be at potential risk, though often unaware of future harm (Drechsler & Kamara, 2021). These uncertainties spark debate about the right level of responsibility. A fault-based negligence standard, such as the “reasonable security” rule in the CCPA, enables courts to assess organizational actions on a case-by-case basis (Almulihi et al., 2022). In contrast, some researchers argue that the ambiguity of cybersecurity and causation calls for strict liability. They suggest holding organizations responsible for breaches gives a stronger incentive to improve security (Alhashim & Rahman, 2021).

To make the negligence framework even more difficult, there is the so-called causation gap. According to Alharbi et al. (2021), the liability of careless organizations can be potentially protected in the event that a more advanced third-party attacker interferes and interrupts the legal path between poor security practices within an organization and the resulting damage. The literature leads to a compromise, therefore, on the agreement that mere importation of the traditional tort doctrine is not enough (Abanumy et al., 2005). It is increasingly believed that a hybrid system, a combination of fault-based principles and proactive governance-focused responsibilities, is the way forward. In this sense, Bygrave (2017) plays a leading role in defining the "accountability principle" of the GDPR as a regulatory form of negligence, making attention to a single breach incident give way to continual, systemic compliance through tools such as Data Protection Impact Assessments (DPIA).

2.2 Comparative Regulatory Paradigms: GDPR and CCPA

It is a theoretical problem of negligence expressed through the diversity of the world's principal data protection regimes (Boudjemaa, 2024). The European Union GDPR offers a risk-based

mechanism. Article 32 of the GDPR states that there should be sufficient technical and organisational measures, and this, as Voigt and Von Dem (2017) discuss, is codification of a developing negligence standard. The factors against which the appropriateness of these measures is judged are the state of the art, cost of processing, and the nature, scope, and context of processing (Suliman, 2025). This system is implemented through the imposition of substantial administrative fines, as well as the right to compensation and either real or non-material damages, as outlined in Article 82. The GDPR has introduced non-material damage with further development in post-GDPR jurisprudence that lowered the burden of proving harm by a considerable margin, thus bypassing one of the major challenges of traditional negligence litigation (Schmitz-Berndt & Schiffner, 2021).

On the contrary, the California Consumer Privacy Act (CPRA/CCPA) is a variant that is more oriented toward consumer welfare. Hoofnagle et al. (2019), as an extrapolation of Federal Trade Commission (FTC) case law regarding unfair and deceptive practices. Its tort of action is precipitated by a failure to execute sensible security processes and practices, and it establishes a de facto negligence threshold that is judged by the civil suit rather than a central body (Awwad & Abdelsattar, 2025). The first weakness identified in the literature is that the original limitation to breaches of specific categories of personal data has resulted in a more limited liability scope compared to the GDPR (Al Harbi, 2025). Finally, whereas the GDPR considers data protection as an essential right, the CCPA tends to act as a consumer market correction mechanism, which represents a philosophical divergence that affects the perception and penalty for negligence.

2.3. The Saudi PDPL: Critical Gaps in the Emerging Discourse

As a nascent law, the Saudi PDPL has only recently begun to attract academic scrutiny, with the emerging literature primarily consisting of descriptive overviews and initial compliance guidance (Alnasser, 2023). A critical gap identified in this review is the lack of in-depth, analytical scholarship that subjects the PDPL to a rigorous negligence-focused analysis using comparative and theoretical frameworks (Almutairi, 2025). The first commentaries, including that of Alhejaili (2024), rightly note that the PDPL establishes general principles of data security without being as granular as Article 32 of the GDPR or the CCPA's trigger for a reasonable security standard. The fact that the law does not specify what constitutes adequate security measures leaves organizations with considerable legal uncertainty. Moreover, the literature has not exhaustively examined the treatment of the two elements of any negligence claim by the PDPL: harm and causation (Alqahtani, 2024). Understanding whether psychological distress constitutes a recoverable harm and how these omissions by a controller can be legally linked to a particular violation is a question that, without a clearly defined statutory framework or a body of judicial precedent, remains unresolved in the Saudi legal literature.

2.4 Theoretical Foundations for Analysing Negligence

The analysis of negligence in the area of data protection law would need to be robust, and to achieve this, a theoretical framework that transcends the text of the statutes would be necessary. This paper will be grounded in three theoretical pillars and will serve as the basis for the analysis. To begin with, Tort Law and Negligence Theory provide the fundamental doctrinal framework for analyzing liability, based on the key aspects of duty, breach, causation, and harm (See Section 2.1). Second, Privacy Theories present conflicting arguments as to why information security is important (Johri & Kumar, 2023). The Liberal Autonomy model considers privacy as the right to privacy and self-determination, which constitute individual dignity, and negligence is treated as the infringement of the right (Ams, 2023). Conversely, Consumer Protection and Structural Power models view data breaches as market failures

or exercises of power, proposing alternative regulatory objectives and solutions (Mashaabi et al., 2023). Lastly, organizational accountability theory posits that successful regulation should not focus on the incidence, but rather on the organizational structures and processes.

This theory plays a crucial role in determining whether a law's motivation encourages the establishment of a genuine culture of compliance, which is a significant issue in discouraging lax enforcement.

3. METHODOLOGY

This research employs a doctrinal legal research methodology, which is qualitative in nature, to systematically investigate the treatment of negligence within the Saudi Arabian Personal Data Protection Law (PDPL). Doctrinal research is defined by its focus on the systematic exposition, analysis, and synthesis of legal rules and principles derived from primary sources such as statutes, regulations, and judicial decisions (Hutchinson & Treščáková, 2022). This approach is uniquely suited to the objectives of this study, as it facilitates a detailed, internal examination of the PDPL's text to identify its core provisions, discern its underlying logic, and critically evaluate its coherence and capacity to define a standard of care for negligence-based data breaches.

3.1 Research Design: Doctrinal Legal Analysis

The core of this research is a doctrinal legal analysis of the Saudi Arabian PDPL. This design was selected because it provides the most appropriate framework for a systematic and authoritative interpretation of the law as it is written. The process begins with a close reading and detailed exegesis of the PDPL's statutory text. The analysis focuses specifically on articles pertaining to the obligations of data controllers and processors, data security requirements, breach notification procedures, and the stipulated penalties and liabilities. The primary aim is to deconstruct the language of the law to determine whether it implicitly or explicitly incorporates the classical elements of negligence, duty of care, breach, causation, and harm, and to assess the clarity of the standard of care it imposes on organizations. This involves examining if the PDPL merely states abstract principles of data protection or if it provides actionable, enforceable standards against which negligent conduct can be measured. The doctrinal analysis forms the foundational layer upon which the critical and comparative evaluations are built, allowing for a grounded assessment of the law's current effectiveness and its doctrinal coherence.

3.2 Data Collection and Sources

The data collection for this study is split into primary and secondary legal sources. The primary sources consist of the authoritative legal texts under examination. This includes the full text of the Saudi Arabian Personal Data Protection Law and its implementing regulations, the consolidated text of the European Union's General Data Protection Regulation (GDPR), and the relevant sections of the California Consumer Privacy Act (CCPA) as amended by the CPRA. These texts serve as the raw material for the doctrinal and comparative analysis, providing the literal provisions from which legal interpretations are derived.

Secondary sources encompass a diverse range of scholarly materials used to contextualize and theorize the findings from primary law. This includes academic books, peer-reviewed journal articles, and commissioned reports from international bodies on data protection law, tort theory, cybersecurity, and comparative legal studies. Special attention is given to literature that discusses the

conceptualization of negligence in digital contexts, the economic and social impacts of data breaches, and the enforcement practices in different jurisdictions. Furthermore, relevant judicial decisions from jurisdictions with more mature data protection litigations are consulted to provide practical perspectives on how courts interpret and apply negligence principles in data breach cases. This comprehensive collection of sources ensures that the analysis is not only textually grounded but also informed by contemporary academic discourse and legal practice.

3.3 Analytical Framework: A Multi-Theoretical Lens

To move beyond a purely black-letter law analysis, this research employs a multi-theoretical analytical framework, as elaborated in Chapter 3, to critically interrogate the PDPL. The analysis is guided by four interconnected theoretical perspectives. First, Tort Law and Negligence Theory provide the classical doctrinal framework for assessing whether the PDPL establishes a clear duty of care, defines what constitutes a breach of that duty, and outlines a coherent path for establishing causation and remedying harm. Second, Privacy Theories (including the Liberal Autonomy, Consumer Protection, and Structural Power models) are used to evaluate the PDPL's underlying philosophy and to frame negligence not just as a legal failure, but as a violation of individual autonomy and a breach of trust. Third, Organizational Accountability Theory shifts the focus from individual acts to systemic and institutional failures, providing a lens to assess whether the PDPL encourages a culture of proactive compliance and risk management within organizations.

3.4 Comparative Legal Analysis

To contextualize the findings from the PDPL and to identify potential best practices, this study incorporates a structured comparative legal analysis with two leading international data protection regimes: the EU's GDPR and the California CCPA. These frameworks were selected due to their global influence, sophisticated regulatory approaches, and their explicit engagement with concepts of accountability, security, and liability. The comparison is focused thematically on three critical areas: (1) how each legal instrument defines and addresses negligence, either directly or through standards of "reasonable security"; (2) the rules and procedures governing data transfer to third countries and entities; and (3) the obligations and timelines for breach notification. By contrasting the PDPL's provisions with those of the GDPR and CCPA, the research aims to highlight relative strengths and weaknesses, identify regulatory gaps in the Saudi law, and distil actionable recommendations for its strengthening.

A critical component of methodological rigor is the language used in the primary sources. For the Saudi PDPL, the official Arabic text published in the Umm al-Qura Gazette is the primary source of analysis. This ensures the most accurate interpretation of legal concepts and obligations. For the comparative analysis, the official English language version of the GDPR and the original English text of the CCPA are used. Where necessary for the PDPL analysis, key terms and provisions were carefully translated by the author, with an awareness of potential linguistic nuances, to facilitate a precise comparison with the English-language frameworks.

3.5 Ethical and Contextual Reflection

This research is a doctrinal study and does not include human subjects. The main ethical concern is to interpret legal texts accurately and in context, while respecting their legal and cultural backgrounds. The analysis takes into account Saudi Arabia's unique socio-legal setting, its developing data protection

laws, and the possible impact of Islamic legal principles. It avoids simply applying outside concepts without careful adjustment.

4. RESULTS AND DISCUSSION

4.1 Doctrinal Ambiguity: The Undefined Standard of Negligence in the PDPL

One of the most significant findings of this study is the conceptual imprecision that surrounds the standard of negligence in Saudi PDPL, revealing a weakness in the regulatory design of its framework. In contrast to the GDPR, which, in turn, conceptualizes negligence in terms of a powerful accountability principle requiring evidence of compliance through Data Protection Impact Assessments, documented records, and risk-based implementation of the notion of appropriate technical and organizational measures. (GDPR, Article. 32), The PDPL imposes a similarly worded but critically hollow obligation.

The fact that the PDPL suggests the need for appropriate technical and organizational measures (PDPL, Article 20) defines an open-textured norm but does not outline it. In contrast to Article 32 of the GDPR, which provides contextual guidelines, such as the level of technological advancement and the cost of implementation, Article 20 does not provide any guidelines, leaving organizations with no clear standard of care. This shortcoming is further exacerbated by comparison with the pragmatic nature of the CCPA approach, which directly associates liability with a lack of either implementing a reasonable security procedure and practice (CCPA 1798.150), which has since been informed by statutory guidelines and case law, and which creates a clearer yet litigious route to proving fault. In its current formulation, the PDPL does not contain any such doctrinal point of reference, and the principle of negligence itself has become an entirely implicit concept, capable of being interpreted unpredictably and post hoc.

This doctrinal ambiguity generates a significant legal vacuum with direct practical consequences for both compliance and enforcement. For regulated entities, the absence of a clearly articulated standard of care, whether based on reasonableness or a dynamic risk-assessment model, fails to provide actionable guidance. Organizations are left to determine their own compliance ceiling, incentivizing a minimalist and self-serving interpretation of "appropriate" measures that may fall short of evolving cybersecurity best practices. To the regulators and courts, the stalemate in determining a clear court test on negligence erodes sound and powerful judgment. In the event of an infraction, the Saudi Data and AI Authority (SDAIA) and legal entities often lack a systematic approach to differentiate between unavoidable security incidents and criminal violations of responsibilities, resulting in the possibility of arbitrariness in the interpretation of the law and legal voids. This uncertainty, in effect, undermines the very purpose of the PDPL in preventive and deterrent agencies, as even the possibility of accidental negligence liability is obstructed by the law's inability to clearly define what constitutes an act of negligence within its framework.

4.2 The Enforcement Gap: Weak Deterrents and Limited Redress

Research shows that the PDPL has a significant enforcement gap, making it less effective at preventing careless data processing (Alnasser, 2025). In contrast, the GDPR and CCPA use stronger, multi-layered enforcement systems. The European model, for example, has a clear and powerful system for issuing fines. These fines can exceed 20 million Euros or 4% of a company’s total yearly turnover if they break the rules (Kärner, 2022).

It does not employ punitive actions but is a logical regulatory tool that directly mirrors the cost of non-conformity, which is directly proportional to the size of a specific organization. The GDPR poses a significant and real financial risk to the company, and consequently causes corporate executives and the board of governance to turn data protection into one of their inherent governance issues and invest in the long-term projects of tight security systems and pervasive compliant programs as an approach that could help avoid expensive reputational and financial damage.

To supplement the regulatory authority of the GDPR, the CCPA addresses a significant aspect of private enforcement, directly empowering individuals. It empowers consumers with a right of action, allowing them to request statutory damages in the event of a breach resulting from an organization's failure to apply reasonable security measures. Such a mechanism is successful in decentralizing enforcement, which leaves a topography of widespread litigation risk. The threat of class-action litigation, where statutory damages can be substantial in cases involving a large number of affected consumers, is a highly effective market-based deterrent. This consumer-empowerment model ensures that accountability is not solely dependent on the resource constraints and enforcement priorities of a central regulatory authority. The PDPL does not have a similar statutory cause of action for persons wronged by careless breaches in the Saudi context. Such an omission deprives the subjects of the data of a clear and easily accessible avenue of redress, leaving the entire task of enforcement to the regulatory body and leaving a vital mechanism of accountability largely unutilized.

The present-day enforcement framework of the PDPL is not robust enough, as it is based on a limited deterrent model. It lacks a multi-faceted structure to integrate the powerful, top-down regulatory fines, such as those under the GDPR, with the bottom-up, market-based pressure of a CCPA-style private right of action. This leads to materially ineffective incentives to deter negligence. Organizations that are run under the PDPL have a reduced perceived risk. Lacking a threat of harsh regulation penalties or a broad-based civil lawsuit, the economic and legal motivation to pursue state-of-the-art security is greatly reduced.

4.3 Procedural Lacunae: Vague Notification Timelines and Accountability Mechanisms

It appears that the framework of the PDPL lacks serious procedural loopholes that prevent effective crisis management and proactive compliance with established procedures. One of its key gaps is that the breach notification requirement towards data subjects is unclearly defined. Although the Implementing Regulations of the PDPL stipulate that notification of data subjects following the occurrence of a breach must be furnished promptly, this is in stark contrast to the GDPR, which has a clear deadline of 72 hours to notify the supervisory authority. Without undue delay is a very ambiguous phrase on its own, which leaves organizations with a dangerous loophole of doubt when they can postpone the important message under the pretext of an internal inquiry or damage survey. Such absence of a defined and strict timeframe to raise an alarm over the concerned people can contribute a lot to the possible damage, given that the concerned individuals would not have a chance to take appropriate measures to curb the impact, such as by freezing their accounts or changing their passwords and treating the effects of a breach. In comparison, the specific time frame of the GDPR is one of reduction, making the vehicle more favorable to the information subject by limiting harm and burdening the data controller with a clear and unambiguous process.

The PDPL establishes general principles but lacks explicit, granular requirements for specific accountability tools, which are the hallmark of modern, prevention-based regimes like the GDPR (Bouderhem, 2024). The principle of accountability under the GDPR is based on Data Protection Impact

Assessments (DPIAs) for high-risk processing and the detailed description of processing operations (GDPR, Articles 35 and 30), which serves as the working principle of the GDPR concept. These are not just administrative activities, but are crucial to compelling organizations to act in an organized manner of identifying, evaluating, and reducing the risks of data protection before they translate into breaches. This lack of such an expressly demanded process that must be documented in the PDPL is a field of strong neglect. It implies that a company can be in compliance with Saudi law, even though it has never conducted a formal, systematic risk assessment of its data processing operations. This is not due to its regulatory culture; an omission contributes to a culture of reactive, rather than proactive, compliance, and makes it extremely challenging to determine whether negligence, as a failure to foresee and mitigate foreseeable risks, existed prior to a breach, because no mandatory paper trail is required to prove due diligence.

4.4 A Hybrid Path Forward: Synthesizing GDPR and CCPA Strengths

A key finding indicates that integrating elements from both the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) offers a more effective approach to improving the Saudi Personal Data Protection Law (PDPL) than adopting either framework in isolation. The study demonstrates that these regulatory models complement each other and collectively provide more robust and comprehensive protection against negligence. The main advantage of the GDPR is that its architecture is designed to be accountability-based and preventive, requiring a culture of compliance to be proactive. Conversely, the CCPA is strong in its ex-post facto, market-oriented deterrence, where individuals can serve as their own attorneys general. A purely top-down regulatory framework, such as the GDPR, may be limited by the supervisory authority's resource base, whereas a purely consumer-litigation framework, such as the CCPA, can result in a lack of uniform enforcement and over-litigation. A middle way is, thus, a better way, both to bridge the enforcement gap and to resolve the doctrinal grey areas found within the PDPL. This synthesis entails the deliberate integration of key aspects from each framework. Based on the GDPR, the PDPL is required to directly address its fundamental tools of accountability by obligating the use of Data Protection Impact Assessments (DPIAs) in high-risk processing and the documentation of processing activities.

These procedures formalize a risk-based model, compelling organizations to document their adherence and critically assess potential harms before they occur, thus providing a tangible criterion of care that was previously lacking. Under the CCPA, the most significant import is the introduction of a legal cause of action for individuals who suffered a breach due to a failure to implement reasonable security measures. This generates a formidable, decentralized punitive response and generates a direct financial outcome of careless conduct that does not rely on the community to implement. Combining the ex-ante procedural rigor of the GDPR with the ex-post-consumer empowerment of the CCPA, the PDPL can establish a regime in which negligence is discouraged by both the daunting threat of major regulatory intervention and the ubiquitous risk of mass-scale private litigation.

4.5 Successful Harmonization and Cultural Legitimacy

Lastly, it is concluded in the analysis that the PDPL has skilfully provided a foundational basis on international interoperability and especially has provided a conditional framework of approaching cross-border data transfers that strategically reflects the principle of adequacy contained in the GDPR, thus providing an indicator that Saudi Arabia is fully prepared to enter the global digital economy while providing a benchmark of data protection to its citizens.

On a more fundamental level, but more importantly, the study reveals that the philosophical foundations of a robust negligence standard are not a transplanted foreign organ but rather deep rooted in the legal and ethical tradition of the Kingdom; the Islamic jurisprudential principles of أمانة-amanah (trust), which instils a fiduciary obligation in the handling of personal information, عدل-adl (justice), which requires the redress of actions that are wrong, and the taboo of ضرر-ḍarar (harm), which forbids inflicting harm on others, have the combined effect of offering a powerful. A synthesis of the foregoing doctrinal and comparative analysis is presented in Table 1 below. This thematic matrix consolidates the critical weaknesses identified within the PDPL's current framework, juxtaposes them against the established benchmarks of the GDPR and CCPA, and directly maps these findings to the specific, evidence-based improvements proposed by this study. The table serves to crystallize the argument that a strategic synthesis of elements from both comparative models is the most viable path to remedying the PDPL's doctrinal ambiguities and enforcement gaps.

Table 1: Comparative Analysis of Negligence and Enforcement Frameworks (PDPL, GDPR, and CCPA)

Thematic Area	**Saudi PDPL (Current Weaknesses)**	**GDPR (Benchmark)**	**CCPA/CPRA (Benchmark)**	**Proposed Improvement for PDPL**
Standard of Care Negligence	Appropriate measures (Article, 20)[1]	Risk-based appropriate measures Article. 32)[2];	"Reasonable security" standard; informed by statutory guidelines and case law.	Incorporate explicit criteria from GDPR [2]Article. 32 and mandate Data Protection Impact Assessments (DPIAs) for high-risk processing to create a

[1]Saudi Data & Artificial Intelligence Authority. (2023). *Personal Data Protection Law (English translation, 2nd rev.)*. Kingdom of Saudi Arabia.
Retrieved from https://sdaia.gov.sa/en/SDAIA/about/Documents/Personal%20Data%20English%20V2-23April2023-%20Reviewed-.pdf.
[2]European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union, L119, 1–88. Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj.
[3]European Parliament & Council of the European Union. (2016). *Regulation (EU) 2016/679 (General Data Protection Regulation) of 27 April 2016 on the protection of natural persons with regard to the processing of personal data…* Official Journal of the European Union, L119, 1-88. Article 82. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A02016R0679-20160504.

	No defined criteria or accountability principle.	Explicit criteria (state of art, cost, risk). Accountability principal mandates DPIAs records.		defined, proactive standard of care.
Enforcement & Deterrence	Limited administrative fines; no clear statutory private right of action for negligence-based breaches.	Strong top-down fines (up to 4% global turnover). Compensation for material/non-material damage (Article. 82).[3]	Bottom-up private right of action for breaches involving lack of "reasonable security"; enables statutory damages via consumer lawsuits.	Adopt a hybrid model: Introduce scaled administrative fines based on turnover (like GDPR) and create a statutory private right of action for breaches due to failure to implement "reasonable security" (like CCPA).
Breach Notification Timelines	Ambiguous "without undue delay" requirement for notifying data subjects.	Strict 72-hour deadline for notifying the supervisory authority.	Specific and reasonable timeframe for notification after discovery of a breach.	Replace "without undue delay" with a clear, definite timeframe (72 hours to the authority, promptly to the data subject) to ensure timely mitigation.
Proactive Accountability Mechanisms	Lacks explicit requirements for documented accountability tools like DPIAs or detailed processing records.	Mandatory DPIAs for high-risk processing; Records of Processing Activities (Article-82)[3]	Focused more on ex-post enforcement rather than ex-ante mandated documentation.	Explicitly mandate accountability tools from the GDPR, specifically DPIAs and Records of Processing Activities, to foster a proactive compliance culture and create a verifiable paper trail.
Philosophical & Cultural Foundation	General principles exist but are not explicitly linked to modern negligence concepts.	Framed as a fundamental right; comprehensive risk-based approach.	Framed as a consumer right; market correction and litigation-driven.	Articulate the standard of care using culturally resonant principles like Amanah (trust) and the prohibition of Ḍarar (harm) to ground the legal duty in Saudi and Islamic legal tradition.

5. DISCUSSION

This study examines how negligence is addressed under the Saudi Personal Data Protection Law (PDPL), using doctrinal and comparative analysis with the GDPR and CCPA as benchmarks. The results show that while the PDPL demonstrates a basic commitment to data protection, it does not yet have the clear definitions, strong enforcement, or detailed procedures needed to prevent, identify, and address data breaches caused by organizational negligence. The main findings regarding doctrinal ambiguity in establishing negligence highlight a fundamental conflict between abstract legal principles and practical considerations.

The standard of care enforcement, as defined by the undefined term 'adequate measures' in the PDPL, makes it both self-referential and legally ambiguous. This observation is consistent with the critique of first-generation data protection legislation, which often emphasizes general guidelines over practical rules (Alsadhan, 2025). However, in the Saudi case, it is especially acute, as there is no established body of judicial precedent to lend the term substance. In developing Alanazi's (2025) observation that the PDPL is overall vague, we will identify the absence of a negligence standard as a critical, narrower defect that disables the preventive role of the law. It is not simply a technical oversight but a fundamental vulnerability that enables organizations to justify poor security practices since the

law does not establish any external standard that they can compare their practice to, such as the state of the art in the GDPR or the reasonableness in the CCPA to which their practice will be contrasted against. The ambiguity serves as a successful defense against negligent behavior because it becomes extremely challenging to demonstrate, a problem that has long plagued tort theory and is exacerbated by a highly complex and opaque data security environment (Memeti, 2024).

The identified enforcement gap further exacerbates this problem, revealing a system with insufficient deterrent power. The finding that the PDPL lacks both the GDPR's scaled administrative penalties and the CCPA's decentralized private right of action is crucial. It suggests that the Saudi regime currently embodies what could be termed a "hollow accountability" model, which imposes obligations without creating credible consequences for their negligent breach. This finding resonates with Hoofnagle et al.'s (2019) assertion that effective data protection requires a "multi-instrumental" approach to enforcement. Our contribution lies in demonstrating how the PDPL's underdeveloped enforcement mechanisms fail to create the necessary economic incentives for compliance. While previous literature has focused on the GDPR's fines (Alhazmi, 2025) or the CCPA's litigation risks in isolation, our analysis highlights the synergistic effect of their absence in the PDPL.

Perhaps the most surprising and significant finding of this research pertains to the foundation for cultural legitimacy. While much of the comparative data protection literature assumes a tension between "global" standards and "local" values, our analysis uncovers a powerful consonance. The discovery that core Islamic jurisprudential principles, الأمانة-Al-Amānah (trust), ` عدل-adl (justice), and the prohibition of ضرر-Ḍarar (harm) provide a robust ethical foundation for stringent data protection duties is a critical insight. These finding challenges narratives that might view the adoption of norms from the GDPR or CCPA as a form of legal transplantation, instead reframing it as a process of doctrinal revitalization and contextualization.

This approach proposes that strengthening the Personal Data Protection Law (PDPL) should emphasize integrating modern data protection into the Kingdom’s ethical and legal traditions, rather than relying on external models. This perspective is consistent with recent scholarship that seeks to ground data governance in diverse philosophical frameworks, while also offering a clear, practical framework for Saudi Arabia and other Muslim-majority countries. The hybrid model represents more than a pragmatic solution; it exemplifies a well-founded regulatory transformation. For instance, combining ex-ante accountability measures, such as Data Protection Impact Assessments (DPIAs) under the General Data Protection Regulation (GDPR), with ex-post-consumer control mechanisms from the California Consumer Privacy Act (CCPA) can mitigate negligence at various stages. This method is distinctive for explicitly integrating two major global approaches, thereby establishing a novel regulatory framework. Furthermore, it advances beyond conventional legal literature that dichotomizes capitalism and legal reasoning, with the GDPR and CCPA serving as exemplars of rights-based and market-based models, respectively.

5.1 Policy Implications

This research identifies key policy issues that necessitate targeted reforms by Saudi regulators. To address gaps in the Personal Data Protection Law (PDPL), new regulations should be implemented. These regulations should establish a reasonable standard of care for data security, utilizing specific risk-based criteria to clarify required measures. Such clarity would resolve existing uncertainty regarding the definition of negligence. Policymakers should also consider introducing a graduated penalty system,

similar to the General Data Protection Regulation (GDPR), to address enforcement deficiencies. Penalties should be commensurate with the severity of the breach and the organization's revenue. Granting individuals a legal right to seek recourse when organizations fail to implement reasonable security measures would support affected parties and promote compliance. Finally, replacing the ambiguous requirement to notify data subjects of breaches without undue delay with a definitive 72-hour deadline would enhance procedural clarity.

6. CONCLUSION

This paper concludes that the Saudi Personal Data Protection Law (PDPL) does not adequately address careless data breaches. Its standards of care, enforcement, and procedures have key weaknesses that limit its ability to prevent and remedy harm. To address these issues, Saudi Arabia should draw on global best practices. This would mean combining the GDPR's proactive, accountability-focused approach with the CCPA's emphasis on litigation and consumer rights. Together, these elements would create a stronger and more reliable system of accountability. Importantly, this legal improvement is not an outside imposition but a logical step forward. The core ideas of duty, responsibility, and preventing harm are already part of Islamic law, including principles like الأمانة-Al-Amānah (trust) and the prohibition of ضرر-Ḍarar (harm). These values give cultural legitimacy to making the PDPL a stronger, more effective, and internationally aligned data protection law for the digital age.

6.1 Limitations and Future Research

While the doctrinal and comparative approach remains fundamental, it is limited by the absence of empirical data regarding the practical application of the Personal Data Protection Law (PDPL) and the compliance challenges faced by Saudi organizations. Furthermore, the lack of domestic judicial or administrative case law from the Saudi Data and AI Authority (SDAIA) restricts analysis to the statutory text, without consideration of its implementation. These limitations, however, highlight clear avenues for future research. Given the evolving regulatory environment, empirical investigations into SDAIA implementation practices and organizational compliance strategies are warranted. Additionally, quantitative assessments of the economic impact of proposed reforms should be pursued. Comparative analysis with other Gulf Cooperation Council (GCC) countries is also necessary to evaluate prospects for regional harmonization. Advancing this conceptual framework through evidence-based research will support the effective development of the PDPL.

Acknowledgements: Not available
Author contributions: The author contributed solely to all parts of this study, including the conceptualization, research design, data analysis, and writing.
Ethical Statement: This doctrinal legal study did not involve human or animal subjects; therefore, ethical approval was not required.
Consent to Participate: Not available
Competing Interests: The author declares that this work has no competing interests.
Grant/Funding information: The author declared that no grants supported this work.
Data Availability Statement: This is a doctrinal research paper without an empirical dataset; all references and materials are either publicly available or cited in the manuscript.
Declaration Statement of Generative AI: Generative AI tools were not utilized in the conceptualization, analysis, or writing of this manuscript. Grammarly was employed exclusively for editing, grammar, and style.

REFERENCES

Abanumy, A., Al-Badi, A., & Mayhew, P. (2005). E-Government Website Accessibility: In-Depth Evaluation of Saudi Arabia and Oman. *Electronic journal of e-government*, *3*(3), 149-156. https://academic-publishing.org/index.php/ejeg/article/view/437/400

Abdullah, A. (2020). *Consumers' personal data protection in Saudi Arabia: A comparative analytical study* (Doctoral dissertation, University of Kansas). ProQuest Dissertations Publishing. https://www.proquest.com/openview/36ca660cf5d8a3728b428d64cefa780b/1?pq-origsite=gscholar&cbl=18750&diss=y

Al Harbi, I. (2025). Artificial Intelligence in Saudi Arabia: Intercultural Human Rights Perspectives on Legal Frameworks and Regulatory Protection (Doctoral dissertation, St. Thomas University).

Al Nafea, R., & Almaiah, M. A. (2021). Cybersecurity Threats in Cloud: Literature Review. *International conference on information technology (ICIT) (779-786). IEEE*. doi: 10.1109/ICIT52682.2021.9491638.

Alanazi, A. (2025). Assessing Clinicians' Legal Concerns and the Need for a Regulatory Framework for AI in Healthcare: A Mixed-Methods Study. *Healthcare*, *13*(13), 1487. https://doi.org/10.3390/healthcare13131487

Aldubayyan, A. (2023). *Privacy regulation of cellular network data: A comparative study with recommendations for the Kingdom of Saudi Arabia* (Doctoral dissertation, The University of Waikato). https://hdl.handle.net/10289/17061

Alfaifi, A. (2024). *Lost profit damages for breaches of commercial contracts: Examining common law and civil law approaches to recovery and lessons for Saudi Arabia* (Doctoral dissertation, University of Essex). https://repository.essex.ac.uk/37771/1/PhD%20Thesis.pdf

Alharbi, A. S., Halikias, G., Rajarajan, M., & Yamin, M. (2021). A Review of Effectiveness of Saudi E-Government Data Security Management. *International Journal of Information Technology*, *13*(2), 573-579. https://doi.org/10.1007/s41870-021-00611-3

Alhashim, S. S., & Rahman, M. H. (2021). Cybersecurity Threats in Line with Awareness in Saudi Arabia. *International Conference on Information Technology (ICIT), IEEE*, (314-319). https://doi.org/10.1109/ICIT52682.2021.9491711.

Alhejaili, M. O. M. (2024). *Securing the Kingdom's e-commerce frontier: Evaluation of Saudi Arabia's cybersecurity legal frameworks.* Journal of Governance & Regulation, 13(2), 275–286. https://doi.org/10.22495/jgrv13i2siart4

Al-Mashaqbeh, Y. A. (2025). Legislative Framework Regulating Digital Media in Jordan and Arab Countries: A Study on The Legal Dimensions. *Lex localis-Journal of Local Self-Government*, *23*(10), 1-20. https://doi.org/10.52152/

Almulihi, A. H., Alassery, F., Khan, A. I., Shukla, S., Gupta, B. K., & Kumar, R. (2022). Analyzing the Implications of Healthcare Data Breaches through Computational Technique. *Intelligent Automation & Soft Computing*, *32*(3). https://doi.org/10.32604/iasc.2022.023460

Almutairi, S. (2025). *Kuwait's fragmented data protection framework: Toward reform through comparative analysis with the GDPR and Saudi Arabia's PDPL.* SSRN. https://doi.org/10.2139/ssrn.5464634

Alnasser, A. (2023). Rhetorical Strategies and Ideologies in Saudi TEDx talks. *International Journal of Linguistics, Literature & Translation*, *6*(3). https://doi.org/ 10.32996/ijllt.2023.6.3.22

Alnasser, H. A. (2025). The Concept of Negligence in Data Breach: A Comparative Doctrinal Analysis of the EU, California, and Saudi Arabia. *Veredas do Direito*, *22*(3), e223404-e223404. https://doi.org/10.18623/rvd.v22.n3.3404

Alqahtani, F. (2024). Persuasion Strategies in Saudi Arabia Vision 2030 Document: A Critical Discourse Analysis Approach. *Theory & Practice in Language Studies (TPLS)*, *14*(4). https://doi.org/10.17507/tpls.1404.32

Alsadhan, A. A. (2025). A Survey of Security Threats and Challenges Related To 5G Networks in Saudi Arabia. *Qubahan Academic Journal*, *5*(3), 474-501. https://doi.org/10.48161/qaj.v5n3a1849

Al-Saggaf, Y., & Weckert, J. (2011). Privacy from a Saudi Arabian Perspective: The case of students in a private university. *Journal of Information Ethics*, *20*(1), 34. https://www.proquest.com/openview/d77227c0f1beaa8d3271d6e8a3d215d6/1?pq-origsite=gscholar&cbl=2035668

Alzahrani, R. B. (2024). An Overview of AI Data Protection in The Context of Saudi Arabia. *International Journal for Scientific Research*, *3*(3), 199-218. https://vsrp.co.uk/wp-content/uploads/

Ams, S. (2023). Blurred Lines: The Convergence of Military and Civilian Uses of AI & Data Use and Its Impact on Liberal Democracy. *International Politics*, *60*(4), 879-896. https://doi.org/10.1057/s41311-021-00351-y

Awwad, A., & Abdelsattar, A. (2025). Digital Evidence in Forensic Accounting-A Study in Saudi Legislation. *Cogent Social Sciences*, *11*(1), 2522958. https://doi.org/10.1080/23311886.2025.2522958

Bouderhem, R. (2024). A review of Saudi e-commerce regulation under the scope of the GDPR. *Arab Law Quarterly*, *1*(aop), 1-19. https://doi.org/10.1163/15730255-bja10154

Boudjemaa, Y. (2024). Ensuring Regulatory Compliance in Cloud-based Big Data Systems: A Framework for Global Operations Adhering to GDPR and CCPA. *Studies in Knowledge Discovery, Intelligent Systems, and Distributed Analytics*, *14*(9), 15-27. https://edgescholar.com/index.php/SKDISDA/article/view/e-2024-09-07

Bygrave, L. A. (2017). Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements. *Oslo Law Review*, *4*(2), 105-120. https://doi.org/10.18261/issn.2387-3299-2017-02-03

Corrales Compagnucci, M., Aboy, M., & Minssen, T. (2021). Cross-Border Transfers of Personal Data After Schrems II: Supplementary Measures and New Standard Contractual Clauses (Sccs). *Nordic Journal of European Law*, *4*(2). https://doi.org/10.36969/njel.v4i2.23780

Drechsler, L., & Kamara, I. (2022). *Essential equivalence as a benchmark for international data transfers after Schrems II.* In E. Kosta, R. Leenes, & I. Kamara (Eds.), *Research handbook on EU data protection* (pp. 314-352). Edward Elgar Publishing. https://doi.org/10.4337/9781800371682.00022

Elgujja, A. A. M. (2020). *Adequacy of the legal safeguards of the patients' confidentiality right under the Saudi Arabian laws* (Doctoral dissertation, University of Salford). University of Salford Repository. https://salford-repository.worktribe.com/preview/1486896/Thesis%2000343621.pdf

Hoofnagle, C. J., Van Der Sloot, B., & Borgesius, F. Z. (2019). The European Union General Data Protection Regulation: What It Is and What It Means. *Information & Communications Technology Law*, *28*(1), 65-98. https://doi.org/10.1080/13600834.2019.1573501

Hutchinson, C. S., & Treščáková, D. (2022). The Challenges of Personalized Pricing to Competition and Personal Data Protection Law. *European Competition Journal*, *18*(1), 105-128. https://doi.org/10.1080/17441056.2021.1936400

Johri, A., & Kumar, S. (2023). Exploring Customer Awareness Towards Their Cyber Security in The Kingdom of Saudi Arabia: A Study in The Era of Banking Digital Transformation. *Human Behavior and Emerging Technologies*, *2023*(1), 2103442. https://doi.org/10.1155/2023/2103442

Kanojia, S. (2023). Ensuring Privacy of Personal Data: A Panoramic View of Legal Developments In Personal Data Protection Law In Saudi Arabia. *J. Int'l L. Islamic L.*, *19*(3), 270-276. https://heinonline.org/HOL/LandingPage?handle=hein.journals/jispil19&div=51&id=&page=

Kärner, M. (2022). Interplay Between European Union Criminal Law and Administrative Sanctions: Constituent Elements of Transposing Punitive Administrative Sanctions Into National Law. *New Journal of European Criminal Law*, *13*(1), 42-68. https://doi.org/10.1177/20322844221085918

Kilovaty, I. (2021). *Psychological data breach harms.* North Carolina Journal of Law & Technology, 23(1), 1–66. https://doi.org/10.2139/ssrn.3785734

Mashaabi, M., Al-Yahya, G., Alnashwan, R., & Al-Khalifa, H. (2023). Arabic privacy policy corpus and classification. In A. Gal, M. Jarrar, & Y. Kanza (Eds.), *Applications of Natural Language to Information Systems* (pp. 94–108). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-35320-8_7

Memeti, N. (2024). From Legislation to Enforcement: Tackling Digital Acquisitions in the Gulf Region. *Digital Society*, *3*(3), 67. https://doi.org/10.1007/s44206-024-00152-9

Nusairat, W. M. (2024). Legal Protection of Personal Data Privacy in the Kingdom of Saudi Arabia. *Manchester Journal of Transnational Islamic Law & Practice*, *20*(1). https://heinonline.org/HOL/LandingPage?handle=hein.journals/jispil20&div=19&id=&page=

Sarabdeen, J., & Moonesar, I. A. (2018). Privacy protection laws and public perception of data privacy: the case of Dubai e-health care services. *Benchmarking: An International Journal*, *25*(6), 1883-1902. https://doi.org/10.1108/BIJ-06-2017-0133

Schmitz-Berndt, S., & Schiffner, S. (2021). Don't tell them now (or at all)–responsible disclosure of security incidents under NIS Directive and GDPR. *International Review of Law, Computers & Technology*, *35*(2), 101-115. https://doi.org/10.1080/13600869.2021.1885103

Suliman, H. O. H. (2025). Evaluating the effectiveness of Saudi Arabia's PDPL in the global digital economy. *Journal of Data Protection & Privacy*, *8*(1), 97-111. https://doi.org/10.69554/ELUX6976

Voigt, P., & Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A practical guide*. Springer International Publishing.

Westin, A. F. (1967). Special report: legal safeguards to insure privacy in a computer society. *Communications of the ACM*, *10*(9), 533-537. https://dl.acm.org/doi/pdf/10.1145/363566.363579

Zuboff, S. (2019). Surveillance capitalism and the challenge of collective action. In *New labor forum*. *Sage CA: Los Angeles, CA: Sage Publications*, *28*(1), 10-29. https://doi.org/10.1177/1095796018819461