AL-BIRUNI

Al-Biruni Journal of Humanities and Social Sciences
Vol. 04, No. 08, 2026, pp. 23-43
ISSN 3104-8900
https://al-biruni-journal.jo

Legal Analysis on Data Breach in the UAE and Its Redress Under the Purview of the UAE Personal Data Protection Law 2021

Irfan Ali [1*]

[1] Department of law, Civil Law, Ahmad Ibrahim Kulliyyah of Laws (AIKOL), The International Islamic University (IIUM), Malaysia. Email: ia.irfan@live.iium.edu.my

* Corresponding Author: IRFAN ALI , ia.irfan@live.iium.edu.my

DOI: https://doi.org/10.64440/BIRUNI/BIR0032

ARTICLE INFO

Article history
Received Apr 26, 2026
Revised May 04, 2026
Accepted July 19, 2026

Keywords

Personal data protection;
data breach;
remedies;
UAE.

ABSTRACT

In the current digitalized post-modern era, technological access to the personal data of natural persons devoid of obtaining consent exacerbates threats to the fundamental 'right to privacy' and self-determination. Protecting the collection, processing, storage, dissemination, and transfer of personal data in the wake of emerging data breaches seeks to safeguard the right to privacy. Following the promulgation of the General Data Protection Regulation (GDPR) in the EU in 2016, the risks associated with data breaches were closely examined, prompting major developing countries worldwide to seek a Personal Data Protection Law for their own jurisdictions, and the UAE is no exception. This article intricately explores the Personal Data Protection Law of 2021, promulgated through Amiri Decree No. 45 of 2021, focusing on the concepts and rights of personal data protection, including remedies for data breaches. The authors offer an in-depth analysis of the ongoing data breach in the UAE and the path toward adopting comprehensive data protection legislation. In this study, the authors expand on the articles of the UAE 2021 law, which serve as the benchmark for the UAE's adequate data protection regulation. The research plan presents a legal analysis of the UAE's approach to the contents of *'personal data protection'* and the *'right to privacy'*, as stipulated in the law. The article alludes to an amalgamation of court proceedings with the stipulated law, evaluating a state data protection legislation reminiscent of the EU GDPR. The scope of the article confines itself to the gaps between theory and practice, including the enactment of the law, the court's methodology for construing it to prevent data breaches, the application of punitive measures, and a legal analysis of how the framework for enacting this nascent law could be implemented.

Al-Biruni Journal of Humanities and Social Sciences
https://al-biruni-journal.jo
Vol. 04, No. 08, 2026, pp. 23-43
ISSN 3104-8900

1. Introduction

Legal theories assess what constitutes consumer harm resulting from a breach of personal data differently: economic theory may recognize privacy costs that legal jurisprudence generally does not. Prior to the proclamation of the Federal Decree-Law No. 45/2021 on the Protection of Personal Data (PDPL 2021), the erstwhile Cyber Crimes Law (also referred to as Federal Law No. 5 of 2012) treated violations of privacy in data breaches as offenses [1]. This law stipulated penalties of up to AED 300,000. Most Data protection officers (DPOs) are unaware of the need to protect personal information shared online, as the advent of Artificial Intelligence (AI) and Chatbot technologies makes all information vulnerable to exposure [2]. DPOs are unable to offer a plausible solution to data protection. For example, in the EU jurisdiction, penalties could be € 20 million or "4 % of the total worldwide annual turnover of the preceding financial years" in certain instances. Notwithstanding, the disclosure of information poses a significant threat to organizations' finances and reputations. Conversely, a study conducted by the Ponemon Institute in the United Kingdom relates that corporations lost 5% of their stock price post-disclosure of data breaches of personal data in their possession, alluding to distrust of the general public [3]. Even a renowned social media platform, like Facebook, was penalized with a hefty fine of £500,000 for a data breach [4]. While the Islamic perspective remains to be further explored, the legal idealogue of damages resulting from Data breach in the UAE is grounded on a firm pedestal, as the laws are enrooted on several regulations protecting the due privacy of netizens, including but not limited to the Penal Code, law no.5 on the Civil Transactions Law of the State of the United Arab Emirates, PDPL 2021 and the Cybercrime Law, are the prelude the development of regulations due to the of Data systems globally [5].

Data breaches are a prerequisite when it comes to critical gaps occurring due to the quantum leap of digitalization in post-modern times, as subsequently compromised data remains vulnerable to use against the personal interests of the general populace. Communication Apps, and social media platforms, such as Facebook, WhatsApp, BOTIM, Instagram, Nord V, X (formerly Twitter), Snapchat, and chatbots of this digitalized age, Microsoft Co-Pilot, ChatGPT, and other AI engines, are widely used for sharing absolute personalized data about the inner privacies of the netizens, through a reconnection with yesteryear buddies. Hitherto, studies reveal that online platforms can influence the lives of

netizens by exposing absolute privacy without obtaining their consent, leading to delinquent social repercussions on the masses [6]. Personal Data breaches create a nuisance; for ulterior motives, cybercriminals exploit confidential data, invade privacy by processing sensitive information, and cause harm by damaging reputations and enabling blackmail through abuse.

This article examines data breaches from a legal and Islamic perspective in the UAE and explores how damages can be awarded to victims through the legal quorum. Subsequently, the article explains the legal rights of netizens to privacy and consent, as well as the research gap regarding damages from online data breaches. Theoretically, the legal theorem is a compound matrix consisting of privacy, legal damages, and data breaches, as the vertices of this matrix [7].

THE DISTINCTIVE NATURE OF PDPL 2021

Limitations

The preparation of a data protection law is a significant benchmark for any jurisdiction, since the Federal legislature of the UAE is bound to implement data protection for all natural persons within its jurisdiction. These efforts include the shift in the protection paradigm toward the right to privacy, which is driving implacable demands for data protection from various angles. However, the authors will be polite to a fault, to evade the enactment of the law for the present and the future, as the enactment of the PDPL 2021 is the crux of the problem. Fundamentally, the legislative authorities must work hand in glove with legal practitioners to improve the efficiency of the law, address subsequent problems, foster greater understanding, and ensure compliance in the public and private sectors alike.

The problem is further compounded by the fact that the definition of personal data, as construed by UAE law, aligns significantly with international benchmark standards, primarily the EUGDPR, yet fails to provide plausible solutions to this development. Personal data covers a wide range of variables, including a natural person's name, identification number, and address. Secondly, the legal problems that could arise could only be curtailed through the power to redress citizens' grievances. The data protection regulations in the UAE protect the data subjects' rights, defining the legitimate, seamless, and transparent processing of personal data and the retention of data for genuine reasons. This notion creates an imbalance between the PDPL 2021 and the general public, as the gap widens drastically, particularly regarding the law's enactment. On the contrary, the data subjects possess the right to access, modify, and delete their personal information. However, these rights are still being

Al-Biruni Journal of Humanities and Social Sciences
https://al-biruni-journal.jo
Vol. 04, No. 08, 2026, pp. 23-43
ISSN 3104-8900

circumvented due to the failure to enact the PDPL 2021. The researcher investigates specific arenas where the PDPL needs significant improvement, as the research identifies these problems and proposes theoretically plausible solutions.

One such factor is the *'purpose limitation principle,'* which confines the processing of personal data to the primary purposes for retention and which, unfortunately, is not legislatively stipulated. Furthermore, obtaining consent clauses should be elevated to an international standard, as the specific terms and conditions for obtaining and revoking consent are not yet clearly defined. Consequently, exceptions are not clearly defined, which exposes the processing of personal data without the data subject's consent to potential harm, especially in matters related to the public interest or medicinal purposes. As these exceptions are imperative, there is a lack of judicial protection to protect the individual rights of natural persons. Thus, offering invaluable insights by addressing a research gap in the theory and enactment of the law is not easy, but it is certainly an impediment that needs to be resolved as soon as possible. This article will try to bridge that vast gap and narrow it down to improve understanding of personal data protection in the UAE, outlining plausible solutions to prevalent problems and proposing consumer redress under the purview of the PDPL 2021, which includes punitive measures for data controllers. Currently, there is no case law on the PDPL 2021. Still, the authors will try to analyze legal case law on damages awarded in 2021, given the lack of case law on the PDPL 2021. Still, the authors will try to analyze the legal issues arising from damages resulting from a data breach.

Punitive measures

Another factor that has become a bone of contention and a key problem is the adaptability of the punitive measures to be applied when a data breach is reported. Unlike its contemporaries, Malaysia's PDPA 2010 and the EU's GDPR, the PDPL 2021, although promulgated as a Data protection law, remains devoid of data breach punitive measures. Subsequently, in response to the UAE legislative body's desire to align with the latest legislation, amendments to specific articles of the Criminal Procedures Law were promulgated through Decree-Law No. 38 of 2022. These amendments may aim to reduce the workload on the courts in the wake of expansive criminal cases, enable criminal dispute resolution at their discretion, ensure justice through uniform procedural rules in subsequent criminal cases, and avoid discrepancies. Under the purview of the Criminal Procedures Law, the UAE legislature subsequently adopted amendments that introduced punitive measures. This paradigm shift alludes to constitutional reformation, albeit awarding legal damages. The challenge, however, is the perception of breaches of criminal

liability in the case of a data breach. This research will hopefully address this gap through legal analysis, in light of the ongoing court proceedings post-2022 in the UAE.

The Extra-Territorial effect

The third most significant research problem is evaluating the extra-territorial effect of the UAE PDPL 2021. A form of extraterritoriality is evident in the PDPL 2021 through the observance of International human rights law, as a subset of public international law, which determines the UAE's extraterritorial obligations to safeguard the fundamental right to data protection. Article (22) of the PDPL 2021, identifying *"Cross-Border Personal Data Transfer and Sharing for Processing Purposes if there is an Adequate Level of Protection,"* explicitly exclaims:

> *"Personal Data may be transferred outside the State In the following cases approved by the Office:*
> *1. If the country or territory to which the Personal Data is to be transferred under special legislation on Personal Data Protection therein, including the most imperative provisions, measures, controls, requirements, and rules for protecting the privacy and confidentiality of the Personal Data of the Data Subject and their ability to exercise their rights, and provisions related to imposing appropriate measures on the Controller or Processor through a supervisory or judicial authority.*
> *2. If the State accedes to bilateral or multilateral agreements related to Personal Data Protection with the countries to which the Personal Data is to be transferred."* [8]

The last prerequisite (non-divisibility) refers to adopting a common denominator as a global standard, through which customer satisfaction may be achieved across global markets via the corporate sector's tech dominance. Data division refers to protecting privacy across multiple jurisdictions through multinational corporate operations, alluding

Al-Biruni Journal of Humanities and Social Sciences
https://al-biruni-journal.jo
Vol. 04, No. 08, 2026, pp. 23-43
ISSN 3104-8900

to heights of excellence. An example of this is the American tech conglomerate Google Inc., based in Mountain View, California, which is implementing European Data Protection principles across its global operations [9]. Finally, by analyzing prevalent factors that serve as prerequisites for embodying the Brussels Effect, whether through de jure or de facto compliance, the corporate sector has significantly altered its compliance with the GDPR [10]. The subsequent genesis observed in EU member states complements the GDPR through specific enactments. It is worth noting that the Brussels Effect enthusiastically disseminated the GDPR's golden principles, thereby establishing a comprehensive legal framework for implementation.

LITERATURE REVIEW

Data protection is a nascent term; the first data protection law was Sweden's Data Act, promulgated in 1973 [11]. The Swedish Data Protection Authority banned individuals and corporations from using information systems to process personal data without obtaining a license [12]. In fact, as a rapidly evolving legal framework that impacts all walks of life, data protection has consumed the authors' focus in recent years. Hence, this study's literature review encompasses pertinent laws regarding information in general and data protection in particular. Since data breaches are a worldwide phenomenon, the literature review includes sources from multiple regions that enacted data protection laws before the UAE.

The development of data protection law in the UAE

Kelvin Bomah brings about a subsequent analysis of the UAE's Dubai International Financial Center (DIFC). His study examines information security and data protection laws in the United Arab Emirates (UAE), with a particular focus on the Dubai International Financial Center (DIFC). Kevin’s paper argues for the urgent need for the UAE Legislature to enact its own data protection law. Kevin mentions the enactment of new cybersecurity laws, which have significant implications for the processing of sensitive data, with a special emphasis on privacy. Regarding cybercrime, the UAE established the National Electronic Security Authority (NESA) to regulate cybersecurity across the federal realm. The PDPL 2021 has brought about significant changes, as Kevin’s 2016 work suggests, by upgrading the judiciary and regulatory framework in the UAE [13]. Kelvin recognized the need for a data protection law and proposed several plausible solutions to its enactment. The UAE data protection framework was proposed and has helped advance the body of knowledge in line with the law. Kelvin’s study illustrates a comprehensive legislative analysis of the law for personal data protection as construed in the GDPR, providing the groundwork for the

requirement for such a law in the UAE to stimulate technical processing. Significantly, a comparative analysis concludes with the civil law jurisdictions of France and Egypt, which serve as precursors to the UAE PDPL 2021 and the common law stipulated by the Dubai International Financial Center (DIFC), emphasizing congruences, albeit strategies through their approaches to the evolution of data protection law in the UAE.

Alshamsi, Obaid Muhayer, and Mohammad Amin Alkrisheh (2024), in their article *"Criminal Settlement Provisions in Emirati Legislation",* discuss the latest amendments to the settlement of criminal cases, enacted through the Amiri Decree Law No. 38 of 2022, as they relate to the Criminal Procedures Law. The newest enactment is indeed a way forward, established after the promulgation of the PDPL 2021, offering an alternative measure within the UAE legislative system. The article analyzes the judicial system's workload and the repercussions of this enactment, which is expected to circumvent time-consuming criminal trials. Furthermore, this article analyzes the definition, scope, and nature of criminal settlement, which may allude to the awarding of damages in the case of a data breach. By adopting non-doctrinal methods, the article identifies misdemeanors amenable to settlement through arbitration, thereby impeding criminal activity. The article explains several crimes that lead to cumulative punitive measures through a misdemeanor brought in a court of law; the public prosecution precedes the case. Furthermore, this article asserts that the UAE legislature ensures settlements for non-incarcerated defendants, thereby circumventing intimidation in the context of free consent. The article concludes by examining the integrity of settlement procedures through conformity with justice in the UAE's legislative framework. This article has helped narrow the gap between punitive realms that UAE courts may adopt as compensation for damages in a data breach situation; other factors highlight a key problem: the adaptability of the ensuing punitive measures to be carried out in case of data breach, as the PDPL 2021, although promulgated as a Data protection law, is devoid of stipulating data breach punitive aspects. Subsequently, in response to the UAE legislative body's desire to align with the latest legislation, amendments to certain articles of the Criminal Procedures Law were recently promulgated through Decree-Law No. 38 of 2022. These amendments may aim to reduce the workload on the courts in the wake of expansive criminal cases, enabling the courts to resolve criminal disputes at their discretion, ensuring justice vis-à-vis uniform procedural rules in subsequent criminal cases, and avoiding discrepancies. Under the purview of the Criminal Procedures Law, the UAE legislature subsequently adopted amendments that introduced punitive measures. This paradigm shift refers to a reformulation of constitutional principles, albeit one that awards legal damages. The challenge, however, is the perception of criminal liability in the case of a Data breach. This research will hopefully address this gap through legal analysis in light of the ongoing court proceedings in the UAE post-2022 [14].

Al-Biruni Journal of Humanities and Social Sciences
https://al-biruni-journal.jo
Vol. 04, No. 08, 2026, pp. 23-43
ISSN 3104-8900

Hasan Younies provides a methodical analysis that highlights data protection, noting that the UAE has comprehensive cybercrime laws; the country's incredible technological advances make its citizens and businesses lucrative targets, as healthcare workers and their sensitive data remain of utmost importance to any country. Hasan's article makes several suggestions but does not conclude with a precise legal solution, as it was written from a scientific standpoint. The authors have noted significant points and proposed plausible solutions within the legal framework of the UAE PDPL 2021, and conclude by presenting the research findings. The author concludes that the UAE legislature has over-burdened itself by doubling its legal efforts to deter emerging cybersecurity risks [15].

AlShamisi (2023) provides an inclusive analysis of the PDPL 2021, examining the scope of the law and the stipulations for processing personal data, including safeguarding privacy, as it discusses data protection in light of the PDPL 2021. It underscores the imperative for conducive legislation and its subsequent promulgation to ensure data subjects' privacy rights. The article further focuses on a critical review of the UAE PDPL 2021 information requirements and federal initiatives in which the primary use is scientific research. The author highlights the fallacy of the incumbent legislative mandate, which should encourage research scenarios, as data processing endures a pragmatic role both for the data processor and the data subject. The juxtaposed analysis suggests that the information prerequisites or compulsory disclosures initiated through application of the UAE PDPL 2021 are short of procedural outputs, containing obstacles for better implementation [16].

Ali Hadi Al-Obeidi and Muaath Sulaiman Al-Mulla, in their article, *"The Legal Basis of the Right to Explanation for Artificial Intelligence Decisions in UAE Law"*, published in the 2022 International Arab Conference on Information Technology (ACIT) through the IEEE, argue intensively, relying on an analytical and descriptive model of the various legislative provisions related to data protection. The findings include that there is no explicit legal provision in the UAE jurisdiction that elaborates on the rights of people holding prerogatives in AI decision-making. Nonetheless, other jurisdictions, including the USA, the EU, and Commonwealth countries, have recognized this imperative right at the international level, in accordance with UNESCO's provisions. The authors recommend that lawmakers at the global and local levels emphasize the right to have AI decisions clarified by recognizing them in explicit, binding legal texts [17]. This article serves as a prelude to AI-based decision-making in the UAE and is widely acclaimed as the way forward for addressing this matter. However, a critical point the authors overlooked is that laws promulgated in the UAE are enacted through Emiri decrees, which are the sole prerogative of the Sovereign governing one of the seven emirates of the UAE. Regarding Federal-level legal provisions, the Ruler of the Abu Dhabi emirate, who is also constitutionally the President of the UAE, holds the prerogative to issue a decree. The

concept of AI decision-making is fairly new in the UAE courts. AI decision-making is also fairly new in the UAE courts, and implementing regulations will take time. Nonetheless, this research will seek to bridge the decision-making gap and develop an AI decision-making framework by offering further recommendations for the way forward to PDPL 2021, including, but not limited to, addressing data breaches arising from the AI regulatory framework in the UAE.

Moustafa Elmetwaly Kandeel, in his paper *"Protecting the information privacy of litigants during remote trials before UAE courts",* published by AAU Journal of Business and Law in Al Ain (2023), elaborates on the aspect of e-litigation in courts, which is an inevitable paradigm shift in court operations at a global scale, imparting technology in litigation in court proceedings. Hitherto, Kandeel explains the reasons for developing an integrated legal framework for conducting an online trial as an adaptive international best practice. He further emphasizes the imperativeness of a remote trial system, as adopted by the UAE courts, enabling the personal data processing of litigants, including defendants, plaintiffs, prosecutors, chamberlains of courts, and victims, as well as the confidential data-subject content of the trial. Furthermore, Kandeel illustrates the significance of implementing a cyber-security framework; deliberations may be conducted through remote trials by obscuring the protection network to prevent data breaches resulting from compromised data privacy. Moreover, Kandeel identifies three imperative findings from his analysis, primarily the prerequisites for remote court proceedings. Secondly, the right-to-information-privacy protection, and lastly, methodology for implementing a remote trial system as an integrated part of UAE court proceedings, while guaranteeing protection of this confidential procedure. This paper has a significant impact on this research, as the authors use a spiral binding to take Kandeel's research to a quantum leap by including further recommendations on the right to privacy and on protecting against data breaches as a way forward for online remote trials [18].

Chemlali, Laroussi, Salmi, Abdesselam, and Benseddik, Leila authored a remarkable paper titled *"A reflection on the UAE's new data protection law: A comparative approach with GDPR,"* published through the Journal of Data Protection & Privacy in 2023. The authors argue that the PDPL 2021 is inevitably influenced by central international privacy and data protection legislation, with the greatest influence coming from the GDPR, and propose evaluating the UAE PDPL through the lens of best international practices. This effort is commendable by imparting the subsequent paradigm shift in legislation for privacy and data protection in the Arab Gulf Cooperation Council (AGCC). The authors adopt a comparative approach by examining key aspects of the PDPL 2021 within the GDPR regulatory framework, providing a set of prerequisites that should be implemented by the corporate sector in the UAE and/or by companies conducting business there [19]. The extra-territorial effect is the focal point of attraction in the PDPL 2021. This research analyzes this aspect

Al-Biruni Journal of Humanities and Social Sciences
https://al-biruni-journal.jo
Vol. 04, No. 08, 2026, pp. 23-43
ISSN 3104-8900

and provides further guidance on its application, offering plausible legal solutions for the article's audience.

Alaa Abouahmed, Moustafa Elmetwaly Kandeel, and Aliaa Zakaria (2024) articulate the significance of protecting personal data and contrast PDPL 2021 with the GDPR, which enshrines rudimentary rights to privacy whilst strictly enforcing confidentiality measures for correspondence. Furthermore, this article illustrates the recognition of personal data protection as a fundamental right by the EU. The article deploys a juxtaposed approach whilst analyzing the legal predicaments of the PDPL 2021 and its relationship to amendments to the GDPR. Although both legal frameworks share common values for protecting personal data, they differ in scope, enactment, and regional background. The incompatibility between the PDPL 2021 and the GDPR is discussed in detail and is therefore quite relevant to this research. Furthermore, the article illustrates jurisdiction of personal data, emphasizing the significance of harmonizing through legal enforcement of both laws across the digital globe [20].

CONCLUSION

Mitigation measures to address the effects

The Arab Gulf Cooperation Council (AGCC) and the EU are stuck in a dilemma; hence, we conclude That Cross-Border data processing transfers fundamental, crucial information between foreign countries and should be discussed through mitigating measures and the repercussions. Such a correlation needs a specific regime based on adequacy judgment, which should educate processors to transfer suitable protections while transferring data; this article highlights these primary modifications through outbound transmission safeguards for sensitive information between the EU and the UAE. The article shows and depicts that AGCC nations like the UAE are much more concerned about the protection of netizens' data, including both citizens and expatriates, and do not want anyone to breach sensitive information, as this is an obligation on a Muslim state to protect its subjects against any harm.

Recommendations

1. The PDPL 2021 should adopt the GDPR's transfer of personal data as a benchmark, where it is strictly and typically prohibited to transfer any data without obtaining appropriate consent.
2. In this regard, it is necessary to understand the three rudimentary benchmarks which are

identified in the GDPR, namely adequacy, suitable safeguards, and decision, which can put an adequacy decision on personal data transfers to a third party, including but not limited to an international organization, because that country or an organization provides protection implicitly. If these prerequisites are not met, the GDPR allows derogations that permit personal data to be transferred to countries only under special circumstances.

3. The transfer may only proceed with the data subjects express desire and given consent and h/she will be that reminded of this particular situation time and again so that there is no data breach which should take place of the sensitive information first.
4. Based on the current findings, this study recommends that the right to protection against subsequent crimes can be done through invasion of privacy through smartphones, as the Pegasus software is designed to infiltrate any retrievable system. Hence, the UAE should not allow publishing about a person's health without their permission.
5. Permissibility of processing information through photographs and other issues should be controlled and only be allowed within the gdpr context, as Islamic law in the UAE does not allow such things to happen. Still, the PDPL does not declare them as any crime whatsoever.
6. Guidelines should be taken from the previous telecommunications law. Under Article 72/2 of this law, the UAE legislative authority indicated that it will certainly penalize eavesdropping on phone calls if permission is not sought from the competent judicial authorities first; this predicament was not implemented through the PDPL
7. but in article 71 of the Emirati telecommunications law it is stipulated that the authorities may penalize any person who has access to the content of a call or telephone message including but not limited to an SMS or an MMS and even WhatsApp and will be penalized according to the issues of data breach article 79 of the same law provides that Emirati legislature uses a broad term that can be applied to any culprit who is involved in eavesdropping or manipulating the privacy of phone calls and disclosing any content of that phone call which would be construed as an illegal action. So such a predicament is definitely a very good opportunity for the PDPL 21 to apply such recommendations

Limitations

The PDPL 2021 is definitely a nascent law and needs a lot of guidance in terms of punitive measures, cross-border data analysis and processing and definitely requires a robustic framework to apply such measures as in the case of the Kingdom of Saudi Arabia and Qatar through the development of data protection laws the awareness of cyberattack risk has further underscored and

Al-Biruni Journal of Humanities and Social Sciences
https://al-biruni-journal.jo
Vol. 04, No. 08, 2026, pp. 23-43
ISSN 3104-8900

force the authorities over there to introduce punitive majors it will stop hitherto the UAE has based its data protection regime entirely on the gdpr which should be common way out but now the crux of the problem which has caused a mega limitation to the processing of the PDPL 21 that the law cannot punish anyone and hence the gap between theory and practice has to be obliterated so that we can move further and establish a legal regime which should help create a unified regional data protection avoiding complacency and accepting international best practices.

Further research directions

Further research should be accompanied through significant researchers specially related to the financial sector where most data breach has caused enormous impounding of financial stress the technological development leading to online platforms where the oblivious public purchases or compromises their data is definitely a matter of concern through tech startups have offered a wide range of practical solutions including several payment platforms and such platforms should definitely be protected through the promulgation of the PDPL 21 in totality in this regard the GDPR's guidance should be taken into consideration as the PDPL 2021 will lacks the legislative framework to accept all financial platforms onto its feel nice and that's why the horizon is definitely suffering payment platforms like buy now, pay later, crowdfunding and peer-to-peer lending across the MENA region has shown significant growth in the number of fintech startups and total revenue investment in these companies exceeds 35 billion U.S. dollars nonetheless there is no guarantee of the protection of personal data whether it be credit cards, debit cards or any other issues in this regard Singapore and her highly reputable bdpa 2012 should be also be taken into action as they have platforms which definitely do not force a person to use their credit or debit cards and information could just be processing financial means through a click which would only be accessible by the person who is trying to conduct this financial discourse. And in the United States of America, the European Union, and Great Britain, this is definitely not a matter of legality but a prerequisite which should not be compromised whatsoever [21].

International Best Practices

Apart from the GDPR and the application of this significant legal framework in the European courts, including French, Italian, and German courts, the UAE has a lot to learn from sister countries, including but not limited to the State of Qatar, the Kingdom of Saudi Arabia, and the Hashemite Kingdom of Jordan. Such data protection regimes have definitely shown more interest in the organization of such data with respect to their users. Here, there is another issue: the number

of UAE data processing units outnumbers any other from her contemporaries, and hence the UAE has a lot on her plate to discuss before the establishment of a robust framework. Still, as they say in English, the night is still young; we have to adopt international best practices not only from the European Union, the United States of America, and Britain but also through Malaysia, Singapore, and the Middle East and North African region so that the best possible solutions could be provided to netizens all across the United Arab Emirates. Overall the UAE has certainly holds the potential to overcome such a situation and has proven in the past to stand tall to all her obligations especially during the 2008 financial crisis when the economy was about to shut down and be obliterated the UAE came forward with a lot of dedication determination and in 2010 came up with the tallest tower in the world the Burj Khalifa and definitely other obstacles were removed so this should be a predictive set to make things go to best and best of accident. The field of personal data protection is definitely a very big challenge for any country, let alone the UAE, and in this regard the UAE can play a significant role through adoption of international best practices all across the world. In conclusion to this article, the author wishes the UAE regime all the very best in promulgating the PDPL 2021 and offering plausible solutions to any data breach problems in the future.

List of Abbrevation: (GDPR): General Data Protection Regulation; UAE: United Arab Emirates; (DPOs): Data protection officers; (AI): Artificial Intelligence; AED: United Arab Emirates Dirham; PDPL: Personal Data Protection Law; EU: European Union; (DIFC): Dubai International Financial Center; (NESA): National Electronic Security Authority; (ACIT): Arab Conference on Information Technology; (AGCC): Arab Gulf Cooperation Council.

Acknowledgements: The author would like to express their sincere gratitude to Al-Biruni Journal of Humanities and Social Sciences - Noor Al-Ilm for Publishing and Distribution for their generous support in waiving all publication fees and facilitating the publication of this manuscript free of charge. Their commitment to promoting scientific research and supporting researchers is highly appreciated.

Author Contribution:

All authors contributed equally to the main contributor to this paper. All authors reviewed and approved the final version of the manuscript prior to submission.

Al-Biruni Journal of Humanities and Social Sciences
https://al-biruni-journal.jo
Vol. 04, No. 08, 2026, pp. 23-43
ISSN 3104-8900

Declaration of generative AI and AI-assisted technologies in the writing process

The authors hereby declare that no generative artificial intelligence or AI-assisted technologies were used at any stage during the preparation of this manuscript, including language editing, proofreading, or content development. The authors take full responsibility for the originality and integrity of the work presented in this publication.

Funding: This research received no external funding. The publication of this article was supported through a full waiver of the article processing charges (APCs) generously granted by Al-Biruni Journal of Humanities and Social Sciences - Noor Al-Ilm for Publishing and Distribution. No financial support was provided for the conduct of the research, data collection, analysis, or manuscript preparation.

Conflicts of Interest: "The authors declare no conflict of interest."

References

[1] Abderrahmane Azzi & Samiya Dakhane, (2022) Social Media and Privacy in the UAE: A Survey Research, University of Sharjah Journal for Humanities & Social Sciences, Volume 19, No. 2 June 2022, **DOI:** https://doi.org/10.36394/jhss/19/2/8

[2] Rossi, A., Kumari, A., Lenzini, G. (2022). Unwinding a Legal and Ethical Ariadne's Thread Out of the Twitter Scraping Maze. In: Schiffner, S., Ziegler, S., Quesada Rodriguez, A. (eds) Privacy Symposium 2022. DPLICIT 2022. Springer, Cham. https://doi.org/10.1007/978-3-031-09901-4_10

[3] Ponemon Institute, "The Impact of Data Breach on Reputation & Share Value: A Study of Marketers, IT Practitioners and Consumers in the United Kingdom," Certify, https://www.centrify.com/media/4772757/ponemon_data_breach_impact_study_uk.pdf (accessed 21 March, 2024).

[4] The ICO, "Facebook Ireland Ltd. Monetary Penalty Notice," ico.org, https://ico.org.uk/action-weve- taken/enforcement/Facebook-Ireland-ltd/ (accessed 21 March, 2024).

[5] Albahar, Marwan, and Mohammed Thanoon. "Privacy Regulations in the Middle East: Challenges & Solutions." (2022). ©2022 International Transaction Journal of Engineering, Management, & Applied Sciences & Technologies, Volume 13 Issue 5, https://tuengr.com/V13/13A5QM.pdf

[6] A. V. Rajan, R. Ravikumar and M. A. Shaer, "UAE cybercrime law and cybercrimes — An analysis," *2017 International Conference on Cyber Security And Protection Of Digital Services (Cyber Security)*, London, UK, 2017, pp. 1-6, doi: https://doi.org/10.1109/CyberSecPODS.2017.8074858

[7] Abderrahmane Azzi & Samiya Dakhane, (2022) Social Media and Privacy in the UAE: A Survey Research, University of Sharjah Journal for Humanities & Social Sciences, Volume 19, No. 2 June 2022, **DOI:** https://doi.org/10.36394/jhss/19/2/8

[8] https://mail.google.com/mail/u/0/#search/Data+Protection+law/QgrcJHsTkKGbCjwkFnLSLWNlmswZtfgSKqB?projector=1&messagePartId=0.1

[9] Gumzej, Nina. "Google Me and Tell Me Who I Am (Not): The Legal Intricacies of Global Delisting Orders in the Right to Be Forgotten Cases." Se. Eur. LJ 12 (2024): 133.

https://access.heinonline.com/HOL/LandingPage?handle=hein.journals/seeljl12&div=10&id=&page=

[10] Seun Solomon Bakare, Adekunle Oyeyemi Adeniyi, Chidiogo Uzoamaka Akpuokwe, & Nkechi Emmanuella Eneh. (2024). DATA PRIVACY LAWS AND COMPLIANCE: A COMPARATIVE REVIEW OF THE EU GDPR AND USA REGULATIONS. *Computer Science & IT Research Journal*, *5*(3), 528-543. https://doi.org/10.51594/csitrj.v5i3.859

[11] Fuster, Gloria Gonzalez. "European Data Protection Law: Don't Let it be (Forever) Misunderstood." In Conceptions of Data Protection and Privacy: Legal and Philosophical Perspectives, pp. 111-128. Hart Publishing, 2026.DOI: https://doi.org/10.5040/9781509983759.ch-006

[12] Naef, Tobias. Data protection without data protectionism: the right to protection of personal data and data transfers in eu law and international trade law. Springer Nature, 2023. https://link.springer.com/content/pdf/10.1007/978-3-031-19893-9.pdf

[13] Bomah, Kelvin. "Information Security and Data Protection: An Overview of Dubai (UAE)." Legal, Ethical & Social Issues in Computing (2016). Legal, Ethical & Social Issues in Computing. https://www.researchgate.net/profile/Kelvin-Bomah/publication/303483760_Information_Security_and_Data_Protection_An_Overview_of_Dubai_UAE/links/57449f1808ae9f741b407e7f/Information-Security-and-Data-Protection-An-Overview-of-Dubai-UAE.pdf

[14] Alshamsi, Obaid Muhayer, and Mohammad Amin Alkrisheh. "Criminal Settlement Provisions in Emirati Legislation." Pakistan Journal of Criminology 16, no. 03 (2024): 1073-1092. **DOI: https://doi.org/**10.62271/pjc.16.3.1073.1092

[15] Younies H, Al-Tawil TN (2020), "Effect of cybercrime laws on protecting citizens and businesses in the United Arab Emirates (UAE)". *Journal of Financial Crime*, Vol. 27 No. 4 pp. 1089–1105, doi: https://doi.org/10.1108/JFC-04-2020-0055

[16] Alshamisi, Mohammad Khamis, Normalini Md Kassim, and Yashar Salamzadeh. "FACTORS INFLUENCING INTENT TO USE AN EDUCATIONAL MANAGEMENT INFORMATION SYSTEM (EMIS): INSIGHTS FROM PRIVATE UNIVERSITIES OF THE UNITED ARAB EMIRATES." Community Practitioner 20, no. 8 (2023): 115-133. https://sure.sunderland.ac.uk/id/eprint/17036/

[17] A. H. Al-Obeidi and M. S. Al-Mulla, "The Legal Basis of the Right to Explanation for Artificial Intelligence Decisions in UAE Law," 2022 International Arab Conference on Information Technology (ACIT), Abu Dhabi, United Arab Emirates, 2022, pp. 1-4, doi: https://doi.org/10.1109/ACIT57182.2022.9994088

[18] Kandeel, Moustafa Elmetwaly. "Protecting the information privacy of litigants during remote trials before UAE courts." AAU Journal of Business and Law 7, no. 2 (2023). https://www.proquest.com/openview/9aa72ab678dd76ab78b0c47c3cbbe52f/1?pq-origsite=gscholar&cbl=5395133

[19] Chemlali, Laroussi, Abdesselam Salmi, and Leila Benseddik. "A reflection on the UAE's new data protection law: A comparative approach with GDPR." Journal of Data Protection & Privacy 6, no. 1 (2023): 24-36. https://www.ingentaconnect.com/content/hsp/jdpp/2023/00000006/00000001/art00003

[20] Abouahmed, A., Kandeel, M. E., & Zakaria, A. (2024). PERSONAL DATA PROTECTION IN THE UNITED ARAB EMIRATES AND THE EUROPEAN UNION REGULATIONS. *Journal of Governance and Regulation*, *13*(1), 195-202. https://doi.org/10.22495/jgrv13i1art17

[21] Sarabdeen, Jawahitha, and Mohamed Mazahir Mohamed Ishak. "Impediment of privacy in the use of clouds by educational institutions." (2015): 167. file:///C:/Users/DELL/Downloads/dubaipapers_662_1.pdf