LEX LOCALIS-JOURNAL OF LOCAL SELF-GOVERNMENT
ISSN:1581-5374 E-ISSN:1855-363X
VOL. 23, NO. S2(2025)

LEGAL SAFEGUARDS FOR E-COMMERCE CUSTOMER DATA UNDER UAE LAW: A DOCTRINAL ANALYSIS OF FEDERAL DECREE-LAW NO. 45 OF 2021

Issa Rabadi[1],Najem Alrabadi[2*]

[1]Department ofCivil Law, College of Law, Fujairah University, Fujairah,United Arab Emirates
https://orcid.org/0000-0002-7340-5514
[2*]Department of Civil Law, College of Law, Middle East University, Amman, Jordan
https://orcid.org/0000-0002-1799-3550

Issa.alrabadi@yahoo.com[1]
n.rabadi@meu.edu.jo[2]

[*]Corresponding Author: n.rabadi@meu.edu.jo

Abstract
This research takes an in-depth evaluation of the law protecting data of the customer's e-commerce activities in the UAE, with particular emphasis on Federal Decree-Law No. 45 2021 concerning the protection of personal data. The study adopts a doctrinal analytical methodology, whereby the researcher investigates obligations concerning digital platforms that must be fulfilled by law, such as requirements of consent, data-minimization, breach notifications, and rights of data access, rectification, and erasure. The analysis also raises key questions as to the legislation's alignment with supranational standards such as the level set out in the General Data Protection Regulation (GDPR), enforceability of the practical rights of data subjects, and compliance obligations of e-commerce operators. The results suggest that the UAE legislation has taken a robust stand with regards to the privacy of digital dealings; however, a certain degree of ambiguity remains with regard to the procedural conditions of implementing such laws, enforcement mechanisms, and cross-border data handling. This works further adds to the discourse on middle-eastern data protection regimes by wholesale portraying the UAE as a possible model of balancing technological advancement with individual privacy rights within the wider context of digital economy.

Keywords: UAE Personal Data Protection; E-Commerce Privacy Law; Federal Decree-Law No. 45 of 2021; Digital Consumer Rights; Data Processing Consent.

Introduction

The Role of E-Commerce in the Digital Economy E-commerce stores are the very backbone of today's digital economy; they operate as marketplaces that offer smooth commercial transactions between business houses and consumers. These interfaces allow very convenient access to product catalogs, pricing methods, purchasing techniques, and different payment systems, thus enhancing the convenience and efficiency of online shopping. This routine collection, storage, and processing of customer data include personal identifiers like names, addresses, and email addresses, and sensitive financial information such as bank credentials and credit card numbers. This information is often provided willingly or solicited upon merit for fulfilling transactions, optimizing services, and complying with requirements. With the advancement of cloud computing, mobile applications, and artificial intelligence, personal data have become tremendously accessible. However, knowing how to access it does not mean it is legal; the unauthorized handling of data without informed, unequivocal consent amounts to a serious contravention of privacy and legal protection.

Interests of Privacy from Commercial and Legal Vantage The personal data that e-commerce businesses collect is not simply operational: it is very much strategic to them. E-commerce platforms have become notorious for data harvesting. The information they gather is used to

optimize marketing algorithms, personalize user interfaces, and sharpen consumer profiling. In less honorable instances, such operations earn them money through transfer or selling of customer data without the consent or knowledge of the data subjects. The commercialization of privacy has generated unease among the public. As pointed out by the Time magazine, an estimated 79% of online shoppers are worried about the way their personal data is getting collected and processed. Such worries evidence the urgent need for legal instruments that would establish boundaries on digital surveillance and data commodification. To address such concerns and align with international best practices, the UAE enacted the Federal Decree-Law No. 45 of 2021 on Personal Data Protection, aiming at an equilibrium between economic innovation and individual autonomy, thereby creating a compliance-based framework for legitimate data governance in digital commerce.

Research Objectives and Methodology In this study, the authors utilize an analytical-doctrinal approach to appraise the evolving UAE law on personal data protection with specific reference to the e-commerce domain.

The analysis centers on Federal Decree-Law No. 45 of 2021; herein open to interpretation, this law is in the context of commentaries, legal literature, and the comparative study of the EU General Data Protection Regulation (GDPR). The objectives of the study are to: (i) identify the legal obligations incumbent on e-commerce platforms; (ii) analyze the applicability and enforcement of consumer rights; and (iii) assess the compatibility of the UAE data protection law with global regulatory trends. Special focus is on customer consent, data minimization, breach notification, and portability rights, further scrutinized under the glass of enforcement issues and vagueness in the regulation. The intent is to ascertain the sufficiency of the UAE legal regime in the protection of e-commerce customer data in a digitizing global economy.

Legal Recognition of Remote Selling Stores in UAE While there is no singular statutory definition provided for e-commerce stores by the UAE legislation, an important step toward their legal recognition was constituted by the 2022 amendment to the UAE Commercial Transactions Law. Article 36 of the amended law, thereby allowing for the definition of commercial establishments in terms such that 'a collection of tangible and intangible assets allocated for carrying out real or virtual commercial activities, whether in technical environments, by means of modern technologies, or traditional methodologies', presents not just a wider legal definition but also clearly welcomes e-commerce platforms under the same umbrella of formal groundings availing them protections under the law of a commercial establishment. This doctrine is furthered in academic literature, with Ameen (2019)defining an e-commerce store as 'a website on World Wide-Web through which services and goods are displayed and purchased via digital interfaces.' Badawi (2015) accentuates the platform architecture, while Al-Shamrani (2018) focuses on the transactional nature of these platforms, referring to the fact that they display goods and complete the purchase process with integrated logistics and payment systems.

Features and Impact of E-commerce Operations on the Consumer E-commerce systems have a broad spectrum of operational features that are meant to not only enhance the consumer experience but also improve business performance. Online shopping allows customers to access a good or services without respect to their location with the multitude of payment modes ranging from cash upon delivery to online secured methods which include Visa, Mastercard, and PayPal, so very easy for these customer transactions.

The platforms also serve as a good data warehouse of consumer insights through reviews, preferences, and profiling behavior which organizations can use to refine their product offerings

and to predict the tide of the market. This constant engagement with customers over social media, promotions via emails, and retargeted ads builds on customer loyalty and sales. Mohammad and Yusuf (2021)emphasize the strategic importance of digital outreach tools such as SEO, email marketing, and advertising based on analytics for visibility and competitiveness for end-user platforms. The above features taken together situate e-commerce at the geographical center of modern consumer behavior and digital business models.

Research Questions

The following research questions are formed to focus on a structure helping tackle specific analytical issues from the main research:

1. How far does Federal Decree-Law No. 45 of 2021 closely relate to international data protection standards; especially, the GDPR?
2. What are the obligations that e-commerce sites have towards the legal regulation for processing personal data in the UAE?
3. To what extent does the PDPL buttress the rights of data subjects on the basis of consent and withdrawal and with consideration of transparency?
4. What are the legal and practical problems that UAE regulators and e-commerce operators face in implementing these provisions on data protection?

This effort critically examines the emerging framework of privacy in digital commerce within the UAE, along with attending doctrinal coherence, regulatory insufficiency, or ambiguity in enforcement.

Literature Review

Legal Regulations for Protecting the Personal Data of E-Commerce Store Customers

The right to privacy, recognized as an international human right, is a foundation for constitutional democracies and international law. Khater (2015, p. 310) correctly comments that privacy pre-existed statutory codification and was acting as a normative bulwark against arbitrary interference. In the UAE, the rapid growth and expansion of digital commerce created a situation wherein e-commerce platforms began to collect vast sensitive information. This category of data spans from biometrics to geolocation, purchasing behavior, financial, and even predictive profiles based on browsing history. The very essence of these broad ecosystems enhances the prospect of surveillance capitalism, incidental disclosure, and discriminatory profiling.

To mitigate these threats, Federal Decree-Law No. 45 of 2021 on Personal Data Protection (PDPL) was instituted by the UAE, adding to the scope of regulation provided through the anti-rumors and cybercrime law. Therefore, a legal framework arises, where unauthorized access is punishable, compliance is made mandatory, and core principles of privacy are elaborated. However, being a new law, it needs to be studied extensively to determine how far it is consistent with international privacy principles and how far it would be responsive to local socio-technical scenarios.

Consent of Client for Processing Personal Data

Consent is the bedrock for the lawful processing of data under the laws of UAE PDPL and similar paradigms like the GDPR. Consent means providing the data subject with an explicit indication of their specific affirmation to the activity in question, but this must be done in a clear and unequivocal manner. Article 6 describes that consent should be informed, documented, and verifiable, while giving the refusal to accept passive acquiescence or tacit acceptance through

inaction. Al-Tahami (2022, p. 413) condemns lax consent regimes, remarking that digital silence or consent marked by pre-checked boxes fails to qualify. The comments made by Al-Khouri (2018, p. 9), which articulate the issues involved, assert that any consent bestowed must substantiate the use of data for a particular purpose, the sharing of data with third parties, and the amount of time that the data will be retained within the holding of those third parties.

Unlike the GDPR, which mandates consent at the highest granular level, that being for each processing purpose, UAE law does not expressly require such purpose-specific consent, paving the way for even broader uses of data under the general terms. The absence of such clarity creates potential overlaps in regulation and confused users, calling for tighter legislative clarity or governmental guidance.

Withdrawal of Consent by the Customer

A right to withdraw consent is also found in Article 6, and thus certain practical ambiguities exist with this right. A person should be able to withdraw consent freely and at any time; however, the law does not lay down the procedural steps to do so. Do we need to make it compulsory for the platforms to provide an opt-out dashboard? Should e-mail notification do? Without prescribed procedures, enforcement is arbitrary and inconsistent. In this way, it stands in striking contrast with Article 7(3) of the GDPR, which states that the controller shall provide an equally easy means of withdrawal as there was to give consent.

In addition, Article 4 of the PDPL creates exceptions to the consent requirement: processing without consent is allowed, where it serves public interest, contractual necessity, or regulatory obligations. Such exceptions would arguably be justified, but when interpreted, they should not be construed broadly to undermine the preeminence of consent as an instrument of informational self-determination. The absence of any balancing testakin to that employed in the assessment of legitimate interests under the GDPRadds to the complexity of the proportionality analysis in these situations.

Processing Personal Data for the Customer's Benefit

Article 4(7) permits the processing of personal data without consent in cases of "legitimate interest of the data subject." However, the clause does not retain definitional accuracy and, therefore, could be interpreted to such degree as to invalidate any effect it may have. Aoun Allah (2019, p. 86)states that the threefold test of necessity, legality, and proportionality must apply in deciding whether or not the processing is to the individual's interest. Article 4(5) also provides for non-consensual processing to occur where public health and national security are concerned. Though such provisions may be in line with international customs during emergencies, they must also be time-bound and have oversight and transparency reports, so as to prevent misuse.

Processing Publicly Available Personal Data

Article 4(2) poses a vexed issue in the context of digital privacy law concerning legally public data. Meheri (2016, p. 12)argues that individuals take on some risk when they voluntarily disclose personal data into public forums or social networks.

Al-Asmar (2019, p. 145)argues that public visibility does not mean unlimited reusability, particularly when profiling or commercial exploitation ensues as the consequence of secondary use.

According to the PDPL, such data can be processed without consent as long as it remains lawful and proportionate. Unlike the GDPR, which tone the user expectation and context-specific integrity (e.g., Article 5(1)(b) on purpose limitation), there is no mention or guidance in the UAE law regarding a secondary use restriction. Such omission would open the floodgates for data

harvesting by e-commerce platforms unless inhibited through executive measures or judicial interpretation.

Substantive Guidelines for Lawful Data Processing

Fair, Transparent, and Lawful Processing

As per Article 5(1), data should be processed in a fair and transparent manner. Thus, fairness entails the unequal treatment of users on the basis of age, nationality, or digital literacy; transparency, on the other hand, entails a proactive disclosure of data handling practices. According to Mohammed (2020, p. 119), acts like a privacy policy that is vaguely worded, obfuscated, or hard to find serve to fail the very threshold of transparency. As Cavoukian (2011) explains in her foundational work on Privacy by Design, the misuse of data beyond its original collection purpose, commonly referred to as "purpose drift", undermines both user trust and legal compliance, violating the principle of purpose limitation embedded in privacy frameworks such as the GDPR and UAE's Federal Decree-Law No. 45 of 2021.

Data Minimization, Accuracy, and Confidentiality

Personal data should be adequate, relevant, and limited to what is necessary with respect to the purpose for which they are processed, as under Article 5 of Federal Decree-Law No. 45 of 2021 of the UAE. Such data needs to maintain accuracy and keep up with changes. In terms of confidentiality, technical measures such as encryption, pseudonymization, and access control need to be applied, among others, for data protection measures (Europol Agency for Cybersecurity [ENISA], 2021). In contrast to Articles 5 and 32 of the GDPR, where this principle fits quite well, DPIAs, however, are not set out at any point as mandatory practices within the UAE PDPL.

Data Retention and Anonymization

According to paragraph 7 of article 5, data should be erased or anonymized once the processing purpose is satisfied, or consents are withdrawn. Anonymization has been defined as rendering data irreversibly non-identifiable, a method which enables secondary usage in research and analytics without compromising individual privacy. But the absence of technical standards of anonymization opens a door for inconsistent applications.

With the purpose of processing fulfilled or withdrawal of a consent of data subject, personal data must be erased or anonymized promptly. By definition, anonymized data is information from which identifiers have been irreversibly removed and thus can be used for secondary research use and analytics ensuring individual privacy. However, the absence of clear technical standards governing the anonymization process poses a risk of ad hoc implementation.

Correction and Deletion of Inaccurate Data

Users are given the right to seek correction or deletion of inaccurate data under Article 5(5) and Article 15. According to Hamisi (2019, p. 61), this is a necessary right for digital dignity whereby, in algorithmic environments, errors in profiling lead to reputational or financial harm. However, lack of specific redress mechanisms or procedural safeguards to ensure timely and effective redress may reduce the practical utility of rights as enshrined in the UAE law.

Findings

It is revealed by this research that Federal Decree-Law No. 45 of 2021 provides a foundational and progressive legal framework for the protection of personal data in the UAE e-commerce sector. The framework has strong normative links with global data protection standards, especially with the European Union's General Data Protection Regulation (GDPR), where the

nutshell idea remains informed consent, data minimization, transparency, breach notifications, and rights of the data subjects. However, this doctrinal examination also points out several weaknesses that affect enforcement and clarity.

The law defines strict legal obligations upon e-commerce platforms, ranging from appointing DPOs to breach notification and institution-level and technical safeguards. These obligations signal a move toward privacy-by-design and institutional accountabilities. However, executive regulations remain vague on the procedural measures for compliance, such as DPIAs, timelines for reporting, and mechanisms of enforcement.

Second, while the law enumerates data subjects' rights (access, rectification, erasure, restriction of processing, objection, and data portability), it is impossible to effectively implement them in practice because procedural standards are too vague. The law does not have concrete guidance on matters like withdrawal of consent, time limits for responding to requests, or formats for data portability, which in practice could lead to these rights being rendered meaningless.

Third, permitting the processing of publicly available data and not limiting further use risks great data abuse in profiling and behavioral advertising. The absence of a contextual or expectation-based analysis akin to the GDPR weakens user protection in open digital environments.

Fourth, the enforcement set-up currently remains far less established than the publicized actions or a system of layers of judicial and administrative remedies and yet it is under the centralized control of the UAE Data Office. This is a diametrically opposed approach, as far as PDPL is concerned, which ensures independent scrutiny, adjudication, and redress by the user. The law is not currently addressing new developments like AI or blockchain, and it is still without any sufficient framework on cross-border data transfers. Hence, lack of responsiveness to the evolving digital ecosystem and interoperability to international systems of data governance are its consequences.

In conclusion, the findings indicate that Federal Decree-Law No. 45 of 2021 has introduced privacy in a much more forward manner for the Gulf region and could best serve as a balancing act between modernization of the economy and data protection. However, the law requires extensive amendments to fulfill all potentials by prescribing detailed executive regulations, overseen in a participatory manner with obvious enforcement and redress provisions in the international standards.

Methods

This is doctrinal legal research, which involves analyzing the components systemic analysis of legal principles: it comprises statutes, case law, and regulatory frameworks with a view to understand and judge consistency in legal principles. This is an ideal methodology for jurisdictions such as the UAE where a new statute, Federal Decree-Law No. 45 of 2021 on Personal Data Protection, is enacted and calls an in-depth exploration to understand its scope, obligations, and chances of enforcement in digital commerce.

The study is based primarily on the original sources, such as Personal Data Protection Law, additional executive regulations, official commentary by UAE legal authorities and published judicial decisions interpreting the rights to privacy and obligations regarding data processing. Such secondary sources supplement this legal infrastructure with doctrinal treatments, peer-reviewed academic articles, and scholarly analysis comparing the UAE with other countries, especially the EU's GDPR.

This study employs a multi-layered approach that enables an assessment of the law through literal as well as purposive interpretive methods. The literal interpretation method analyzes

statutory language, such as "consent"," data minimization", and "anonymization", whereas the purposive method puts those provisions into broader public policy purposes, such as encouraging digital innovation without sacrificing user autonomy.

Further, as much as possible, this doctrinal analysis tries to enhance practical value through concrete references to case precedents and regulatory rules from other similar legal systems like the Article 29 Working Party opinions of the GDPR, enforcement actions by the UK Information Commissioner's Office, and interpretive rulings from GCC member countries. These comparisons demonstrate divergence and space under which legal harmonization can take place.

Next, for example, the methodology generates hypothetical situations and doctrinally plausible interpretations of such actions as unauthorized sales of data, vague withdrawal of consent, and transfers of data across borders for the case study under UAE's provisions. This makes the analysis relevant in real co-commerce practices and makes it practical for both scholars and practitioners.

Results

The findings brought forth from this research have demonstrated a complex and thorough regulation under the UAE federal decree law no. 45 of 2021 regarding the entire life cycle of personal data processing in e-commerce contexts. The framework would not only impose technical and organization responsibilities on data controllers; it would also give consumers rights that are in close correspondence with international standards such as those, which are intrinsic in the General Data Protection Regulation (GDPR). The text speaks about structural legal obligations for e-commerce platforms and the actionable rights of data subjects under the law.

Legal Obligations for E-Commerce Platforms

Appointment of Data Processors

As per Article 7 of the PDPL, e-commerce platforms are expected to appoint qualified data processors formally. Such data processors shall be responsible for processing personal data strictly following the instructions from the controller. Further Article 8 requires such a relationship to be regulated by a binding legal agreement sufficing nature, purpose, lifespan, and categories of the data to be processed in it. Such an arrangement of delegation separates operational works from governance accountability. Using such an illustration, Noon.com, as an example of a marketplace, can outsource data analytics but would be held ultimately responsible for the lawful use and protection of personal data. Thus, ensuring that there are clearly set performance metrics and regulatory expectations.

Oversight by Data Protection Officers (DPOs)

Article 11 mentions the need for Data Protection Officers (DPOS) from organizations that process huge volumes of sensitive data. The DPO would Internally monitor compliance and would assist in conducting risk assessments as well as act as an interface with the relevant data protection authority. Its qualifications must reflect technical competence and legal knowledge, especially in cybersecurity, privacy law, and data lifecycle management. The law emphasizes institutional oversight, for companies that do not appoint or empower DPOs will face sanctions. The presence of a DPO also has the effect of enhancing users' trust since it indicates the commitment of the organization toward data protection.

Breach Notification Duties

Article 11 mentions the need for Data Protection Officers (DPOS) from organizations that process huge volumes of sensitive data. The DPO would Internally monitor compliance and would assist in conducting risk assessments as well as act as an interface with the relevant data protection authority. Its qualifications must reflect technical competence and legal knowledge, especially in cybersecurity, privacy law, and data lifecycle management. The law emphasizes institutional oversight, for companies that do not appoint or empower DPOs will face sanctions. The presence of a DPO also has the effect of enhancing users' trust since it indicates the commitment of the organization toward data protection.

Data Security and Confidentiality Measures

It is not enough to make appointments and report obligations; rather, e-commerce entities are expected to put in place strong technical and organizational safeguards such as end-to-end encryption, pseudonymization, access controls, and conduction of regular penetration tests. Implicitly, the law gives a leeway for privacy-by-design principles encouraging platforms to consider the implications of data protection in the lifecycle of developing digital services. Non-compliance does not only expose a firm to legal liability but also damages the firm's reputation in an increasingly consumer-savvy digital world where consumers care more about privacy issues.

These not only amount to some appointment and reporting obligations but also require formulation and application of strong technical and organizational safeguards for e-commerce entities such as end-to-end encryption, pseudonymization, access controls, and regular penetration testing. The law implicitly encourages the taking of principles of privacy-by-design, which suggest that platforms should integrate data protection into the development lifecycle of digital services. Noncompliance would not only expose a firm to legal liability but also damage its reputation among today's waning consumer-base where consumers are increasingly concerned about digital privacy.

Data Minimization and Purpose Limitation

Even the PDPL indicates that only such data should be collected and processed, which is strictly necessary for the declared purpose. Although e-commerce platforms ask for a number of demographic information, device metadata, and behavioral data, they are now required to prove the importance of each data collation. Article 5(3) establishes the processing to be proportionate and only for such purposes as were determined before, thus limiting the exposure to misuse or repurposing. This principle is in direct contrast to the most common practice where users are profiled for advertisement targeting without their consent.

Rights of Data Subjects

Transparency and Access Rights

Article 13 presents that the data subjects shall be informed of the types of data collected, the purpose for collection, the period of retention, whether data collection is to a third party, and whether it is transferred abroad. It advocates for transparency as the tool to enable informed decision-making and autonomy in the user. Controllers are to provide all necessary information on this front during the collection of data. This is mostly by way of privacy notices embedded in online checkout, registration forms, or cookie consent banners.

Right to Data Portability

It gives users mobility or the right to move their data from one platform to another under Article 14. The enhancement here is competition and free user choice within markets where providers

personalize service experience based on historical data. However, in contrast to the GDPR, there is no specific provision in PDPL about data formats or timelines for transfer or interoperability requirements that make this right functional. Thus, this provision is still developing and will need regulatory guidance to be made functional in practice.

Right to Rectification and Erasure

Article 15 gives users the right to rectify inaccuracies and to request deletion of data in some instances. This is relevant in cases where the original purpose for the processing is no longer valid; where an individual has withdrawn their consent for the processing; or where the processing was unlawful. There are exceptions where data must remain in order to meet public interest objectives or for legal claims. A customer may, for instance, ask for the deletion of his or her transaction history but be denied if the platform needs it for audit purposes. The platforms are also under an obligation to act "without undue delay"; in this regard, "undue delay" conveys a sense of urgency in addressing the grievance of the data subjects.

Right to Restriction and Objection

Articles 16 and 17 confer on data subjects various and intricate rights to restrict processing or to object to it. Restrictions will come into play upon challenges to the accuracy of the data or in cases of unlawful processing, meanwhile objections will apply in scenarios of direct marketing or profiling. These provisions are especially salient in e-commerce contexts where targeted advertising and customer segmentation are the norms. Consumers must have mechanisms at their disposalsuch as real choice to opt out and or perhaps user preference dashboardsthat will allow applying these rights in practice.

Procedural Implementation of Rights

Although the law grants these rights, their procedural application is still somewhat uncertain. For instance, users may encounter inaccessible means for requesting data, ambiguous opt-out procedures, or no redress at all. Executive regulations would have to define the format, timeline, and enforcement mechanisms so that these rights may be exercised and will not remain just an empty promise.

Redress and Remedies

Provides a right to submit complaints to the data protection authority and seek judicial remedies. Unfortunately, there is no provision for a separate supervisory body similar to GDPR's DPAs-or standardized timelines for the resolution of complaints. Therefore, until those institutions are operational, redress may remain fragmented and undoubtedly depends on the larger orbit of civil or criminal judicial processes. In principle, the peculiar legal regime gives a blueprint for privacy protection in e-commerce, indicating an admirable attempt to globalize itself. However, in practice, these rights and obligations require serious enforcement and meticulous procedural laying down for their realization in the routine activities of digital commerce, while the rights given to the users denote a maturing best-practice model in the Gulf Arab region. The legal framework itself is robust. However, much needs to be done practically in terms of engaging with the development of executive regulations and bringing clarity to their interpretation.

Discussion

This study finds that the Federal Decree-Law No. 45 of 2021 (PDPL) becomes a great leg-up in the country’s fast-growing e-commerce sector concerning the legal infrastructure for the protection of personal data. Hence, it takes a rights-based approach by recognizing worldwide privacy principles of lawful processing, data minimization, consent, breach notification, access,

rectification, and portability. Our studies show that although the PDPL aligns conceptually with international systems like the European Union-based General Data Protection Regulation (GDPR), some procedural vagueness's, lack of institutional clarity, and technological blindness impede its full operationality. This paper contributes to the growing body of research advocating for data protection frameworks that not only mirror global best practices in form but are equally effective in enforcement and contextual adaptability.

The doctrinal analysis revealed critical gaps in the PDPL's execution framework. While Article 6 enshrines the right to withdraw consent at any time, it remains silent on how such withdrawal should occur: whether verbally, digitally, or via platform dashboards. This ambiguity poses challenges for both consumers and e-commerce providers, leading to potentially inconsistent compliance practices and dilution of user autonomy. Clarity in digital consent mechanisms is essential for the effective protection of data subjects' rights in e-commerce environments, especially in civil law jurisdictions such as the United Arab Emirates, where procedural flexibility is constrained by codified legal norms. The absence of explicit procedures for withdrawing consent undermines legal certainty and may compromise individuals' control over their personal data (Federal Decree-Law No. 45 of 2021).

A similar challenge arises in Article 14 regarding data portability, which lacks implementation guidelines concerning interoperable formats, timing, or platform responsibility in effecting data transfers. The PDPL stipulates the UAE Data Office as the regulatory authority, but conspicuously, no enforcement actions are publicized, and transparency is wanting in procedures and guidelines for complaint resolution or remedies. This centralization may expedite political harmonization but probably reduces public accountability and trust if no participatory oversight is established.

Moreover, while the PDPL gestures toward regulating publicly available data (Article 4), it does not contextualize different types of public disclosures, such as data shared on social media versus data scraped by third parties for profiling. Dewi et al. (2024) find that poorly designed AI interfaces can reduce user autonomy and consent validity, particularly in mobile commerce, where users may unintentionally authorize broad data uses through dark patterns or non-transparent cookie banners.

The PDPL also omits direct provisions for rapidly emerging technologies like AI, real-time tracking, or biometric profiling, despite their increasing prevalence in UAE e-commerce. Where necessary protections against automated decision-making are not provided, or if there are no provisions for explanation and human review (as stipulated under Article 22 of GDPR), consumers remain subject to the obscuration of algorithmic operations and resultant discrimination. Such gaps present a compelling case for interpretive development either through executive rules or judicial pronouncements to clarify uncertainty and guarantee vigorous enforcement.

Our findings align with a growing body of literature calling for enforceable and contextually responsive data protection frameworks. Otieno (2025) noted that regulatory effectiveness hinges not only on codifying user rights but also on the presence of institutional enforcement and sectoral adaptation. Shen (2025)similarly argued that laws failing to bridge the gap between statutory language and digital realities remain ineffectual in safeguarding user privacy.

Ardika (2025), examining Indonesia's PDP Law, found that despite legal mandates, weak enforcement and public unawareness rendered users unprotected. The UAE, though more centralized, reflects similar vulnerabilities. Ibrahim et al. (2025) reinforce these concerns from a

cybercrime angle, observing that the UAE's electronic fraud laws lack precedent-setting enforcement mechanisms.

Further insights come from Wiwoho et al. (2024), who advocate for open APIs and mandatory data format standards to operationalize the right to data portability. The UAE currently lacks such technical underpinnings. Li et al. (2025) argue for AI-specific regulatory guidance in the GDPR, especially concerning legitimate interest claims. The UAE's silence on this issue risks repeating Europe's legal uncertainty.

Finally, Godbole (2024) and Gopal et al. (2025)propose frameworks for ethical and trust-centric design in e-commerce personalization and customer service, cautioning that unchecked AI implementation can erode user privacy. These insights are vital for a market like the UAE, where AI chatbots and personalization engines are rapidly being integrated into retail platforms.

E-commerce platforms in the UAE must proactively develop internal mechanisms that anticipate PDPL enforcement. These include privacy dashboards, consent withdrawal tools, and breach notification protocols. The UAE Data Office must issue executive regulations that define timelines, consent modalities, and redress processes. Sector-specific codes of practice, developed in collaboration with legal scholars, technologists, and civil society, could foster adaptive compliance. The legal gaps in AI governance must be addressed. The UAE should consider clauses akin to GDPR's Article 22, as well as require DPIAs for high-risk technologies. Fourth, clarity on international data transfer mechanisms is needed. Without mutual recognition mechanisms, UAE-based multinationals may face compliance bottlenecks. Fifth, a public education campaign in Arabic, English, and other regional languages should be launched to bridge the awareness gap.

This study's strength lies in its doctrinal method combined with cross-jurisdictional comparison. The integration of AI concerns, procedural clarity, and institutional accountability enriches the analysis and offers actionable insights for both scholars and policymakers.

Given the PDPL's recent enactment, its full implementation remains incomplete. There are no judicial interpretations or large-scale enforcement precedents available. While comparative insights are valuable, the UAE's civil law system and centralized enforcement model limit direct transplant ability from EU examples.

Future studies should track executive regulations, investigate consumer and business experiences under the PDPL, and explore legal-technical integration points such as blockchain-based consent management. Comparative analysis with Saudi Arabia, Qatar, and Bahrain will be vital for shaping regional convergence. Additionally, interdisciplinary work involving legal scholars, designers, and engineers could pioneer regulatory tools that are not only compliant but also human-centered.

Farooq et al. (2024) offer a model for AI-based fraud detection frameworks that balance innovation and consumer rights. Their emphasis on ethical design, algorithmic transparency, and participatory oversight could inform UAE policy in regulating AI within e-commerce.

Taken together, these findings underscore the UAE's significant legislative ambition in data protection. However, real progress requires procedural clarity, regulatory transparency, and anticipatory adaptation to new technologies. The PDPL offers a foundation, but its success will depend on execution, interpretation, and the creation of a participatory data governance culture that centers user dignity and systemic accountability.

Conclusion

Through the present study, it has been demonstrated that the Federal Decree-Law No. 45 of 2021 of the UAE lays down a very comprehensive and forward-leaning legal framework for protection of personal data in the e-commerce setting. A doctrinal legal analysis shows that the law incorporates globally understood privacy principles like informed consent, minimization, access rights, breach notification, and portability in a structure that fits with the UAE digital economy. By doing this, the study highlights the efforts made and the existing gaps in the approach adopted by the UAE in the context of digital consumer protection based on critical assessment of statutory provisions, judicial interpretation, and comparative norms (chiefly GDPR).

While it describes the legal architecture as being strong after the study, the recommendations highlight areas for further development. Among main issues are procedural ambiguities that have appeared regarding the enforcement of rights in relation to withdrawing consent and data portability. Without clear executive guidance on operationalizing these rights, there is a potential of the rights being defeated. It also proposes enhancing participatory oversight and interpretive transparency, given the increasingly relaxed approach adopted by the law with respect to the use of publicly available information and the centralized enforcement model.

All in all, the PDPL is a landmark in regional governance of privacy and gives the UAE a fair chance to take the prime position in regulatory setting of Middle East standards for data protection. The proposed UAE data protection regime, if properly implemented and supported by targeted regulatory instruments, building institutional capacities, and engagement of stakeholders, could be a model in the balancing act between the economic modernization and ethical stewardship of data. This research, with its findings and recommendations, is aimed at enhancing compliance and trust in consumers and contributing to the regional discourse toward harmonizing digital laws with international best practices.

Recommendations

To sharpen and streamline measures aimed at enhancing compliance and trust in the UAE's data protection regime, particularly within the e-commerce sector, several actions are recommended. First, there is a need to rapidly enact executive regulations that determine the principal rights, procedures, and law enforcement aspects under Article 28. Second, serious offences should be criminalized through the introduction of penalties for intentional breaches, thereby strengthening accountability efforts. Third, objection rights must be augmented by enabling individuals to bar intrusive processing on grounds of public interest. Fourth, targeted advertising without consent should be prohibited, ensuring that no advertising data is used without obtaining explicit permission. Finally, building public awareness is crucial, and this can be achieved through a nationwide campaign to educate consumers about their rights.

Conflict of Interest

The authors confirm that there are no conflicts of interest.

References

Godbole, R. (2024). *Implementing ethical data practices in e-commerce personalization: A technical framework*. *International Journal for Multidisciplinary Research, 6*(6). https://doi.org/10.36948/ijfmr.2024.v06i06.33524

Ameen, S. T. (2019). *The legal system of e-commerce*. Dar Al-Matbuat Al-Jamia.

Mohammad, R., & Yusuf, M. (2021). *Application of the legal system of commercial establishments to e-commerce websites*. *Journal of Sharia and Law, UAE University*, (67).
Al-Tahami, S. W. (2022). *Regulations for processing personal data: A comparative study between French law and Kuwaiti law*. *Journal of the International College of Kuwaiti Law*, *41*.
Al-Shamrani, A. B. (2018). *The legal system of e-commerce stores*. Dar Al-Ilmiyya International for Publishing and Distribution.
Badawi, K. (2015). *Websites design*. Dar Al-Kutub Al-Ilmiyya for Publishing and Distribution.
Al-Khouri, A. M. (2018). *Data privacy and protection of individual identity in the digital world*. Paper presented at the Gulf Cooperation Council Forum for Electronic Community Engagement and Digital Governance, Abu Dhabi, UAE.
Aoun Allah, H. A. (2019). *Provisions of confidentiality of private information*. Al-Wafa Legal Library.
Khater, S. Y. (2015). The right to access personal data in France. *Journal of the Kuwaiti International College of Law, 3*(9), 279–394.
Al-Asmar, A. (2019). *Protection of private life in light of the development of information technology* (Doctoral dissertation, Ain Shams University, Faculty of Law).
Mohammed, A. B. (2020). *The legal regulation of personal data processing*. Dar Al-Nahda Al-Arabiya.
European Union Agency for Cybersecurity (ENISA). (2021). *Guidelines on pseudonymisation techniques and best practices*. https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices
Dewi, Z. Y. A., Saskirana, A., & Hidayat, F. R. (2024). Pengalamanpengguna e-commerce berdasarkanpemanfaatan AI. *JATI, 9*(1). https://doi.org/10.36040/jati.v9i1.12517
Otieno, E. A. (2025). Data protection and privacy in e-commerce environment: Systematic review. *GSC Advanced Research and Reviews, 22*(1), 24–36. https://doi.org/10.30574/gscarr.2025.22.1.0024
Shen, Z. (2025). *Study on countermeasures for the protection of consumers' personal information rights from the perspective of civil and commercial law*. https://doi.org/10.71222/t48vgv55
Meheri, A. H. (2016). *Protection of personal data and individual privacy: A comparative study of legal regulations in the European Union and Algeria*. Paper presented at the E-commerce Adoption Conference in Algeria.
Ardika, I. W. C. (2025). Tinjauanhukumterhadapperlindungan data pribadi di era digital: Kasus kebocoran data penggunalayanan e-commerce. *Indonesian Journal of Law and Justice*. https://doi.org/10.47134/ijlj.v2i3.3601
Hamisi, R. (2019). *Legal guarantees for the protection of personal data in the digital space*. Paper presented at the Third International Conference on Law and Justice, International Islamic University Malaysia.
Ibrahim, E., Sharif, H., &Aboelazm, K. S. (2025). Electronic fraud in the United Arab Emirates legislations. *Journal of Lifestyle and SDGs Review*. https://doi.org/10.47172/2965-730x.sdgsreview.v5.n02.pe04040
Wiwoho, J., Pati, U. K., & Pratama, A. M. (2024). Enabling data portability and interoperability under Indonesia's data protection law. *Masalah-Masalah Hukum, 53*(3), 279–290. https://doi.org/10.14710/mmh.53.3.2024.279-290

Li, W., Li, A. Z., Zhang, Y., & Zheng, Q. (2025). *Submission to the European Data Protection Board's public consultation on the 2024/01 guidelines on legitimate interest under the GDPR*. SSRN. https://doi.org/10.2139/ssrn.5029217

Gopal, R. (2025). The impact of AI-powered chatbots on customer service and conversion rates in e-commerce. *EEL Journal, 15*(1). https://doi.org/10.52783/eel.v15i1.2392

Farooq, A., Abbey, A. B. N., &Onukwulu, E. C. (2024). Conceptual framework for AI-powered fraud detection in e-commerce. *WJARR, 24*(3). https://doi.org/10.30574/wjarr.2024.24.3.3961

Cavoukian, A. (2011). *Privacy by design: The 7 foundational principles – Implementation and mapping of fair information practices*. Information and Privacy Commissioner of Ontario. https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf

United Arab Emirates. (2021). *Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data*. https://www.uaelegislation.gov.ae/en/legislations/1972/download