PERSONAL DATA PROTECTION IN THE UNITED ARAB EMIRATES AND THE EUROPEAN UNION REGULATIONS

Alaa Abouahmed *, Moustafa Elmetwaly Kandeel **, Aliaa Zakaria **

* *Corresponding author*, College of Law, United Arab Emirates University, Al Ain, UAE;
Faculty of Law, Helwan University, Cairo, Egypt
Contact details: College of Law, United Arab Emirates University, P. O. Box 15551, Al Ain, UAE
** College of Law, Al Ain University, Al Ain, UAE

How to cite this paper: Abouahmed, A., Kandeel, M. E., & Zakaria, A. (2024). Personal data protection in the United Arab Emirates and the European Union regulations. *Journal of Governance & Regulation, 13*(1), 195–202. https://doi.org/10.22495/jgrv13i1art17

ISSN Online: 2306-6784
ISSN Print: 2220-9352

Received: 12.06.2023
Accepted: 30.01.2024

JEL Classification: K10, K15, K19, K24
DOI: 10.22495/jgrv13i1art17

Abstract

In our digital age, the exchange of personal data has become an integral part of daily life, with smartphones and the internet serving as conduits for this information. However, this practice brings forth many legal complexities concerning data privacy, highlighting the need to safeguard personal information. This research explores the significance of protecting personal data while drawing parallels with the fundamental right to privacy and the confidentiality of correspondence (Ali, 2021). Moreover, the study delves into the European Union's (EU) acknowledgment of personal data protection as a fundamental right. It employs a comparative analytical approach to scrutinize the implications of Federal Decree Law No. 45 of 2021 and its relationship with the amendments introduced to the European General Data Protection Regulation (GDPR) in 2018. Despite both legal frameworks sharing the overarching objective of safeguarding personal data, they diverge in terms of scope, applicability, and regional context. These distinctions may potentially give rise to challenges and incompatibilities. This research highlights the evolving landscape of data protection and underscores the increasing importance of achieving harmonization and compliance in our interconnected world (AlShamisi, 2023).

Keywords: EU, General Data Protection Regulation, The United Arab Emirates, Right to Privacy, Personal Data, The Organisation for Economic Co-operation and Development Guidelines

Authors' individual contribution: Conceptualization — A.A., M.E.K., and A.Z.; Methodology — M.E.K. and A.Z.; Resources — A.A., M.E.K., and A.Z.; Writing — Original Draft — A.A., M.E.K., and A.Z.; Writing — Review & Editing — A.A., M.E.K., and A.Z.; Supervision — A.A.; Project Administration — A.A. and M.E.K.

Declaration of conflicting interests: The Authors declare that there is no conflict of interest.

Acknowledgements: The Authors would like to extend their gratitude and appreciation to all who have helped carry out this paper, and to all who have provided any facility to complete this work.

1. INTRODUCTION

This research examines the protection of the privacy of personal data that are processed electronically. Electronically processed personal data is defined as "any information relating to an identified or identifiable natural person" by Article 4(1) of the General Data Protection Regulation (GDPR). The rules stipulate that any law should provide a precise and unambiguous definition of sensitive personal data and the degree of protection should be commensurate with the sensitivity of each category of data (e.g., genetic and biometric data).

The United Arab Emirates (UAE) legislator defined personal data as: "any data relating to an identified natural person, or a natural person who can be identified, directly or indirectly, through the linking of data, by using elements of definition such as his name, voice, image, identification number, online identifier, geographical location, or one or more physical appearance characteristics, physiological, economic, cultural or social characteristics, including sensitive personal or biometric data" (Federal Decree Law No. 45/2021 on the Protection of Personal Data, 2021, Article 1).

The UAE legislator demonstrated prudence by maintaining consistency between the definitions in its data protection laws and those outlined in the GDPR. This consistency is particularly notable in the context of defining personal information, encompassing elements such as a person's name, identification number, location, specific physical, biological, genetic, or mental factors, economic, cultural, or social (Sethu, 2020).

Especially since to implement the protection frameworks for such data, it is necessary — according to the GDPR — that the data should be clearly defined and include genetic and biometric data because it reveals personal characteristics that have a lot of sensitivity and be given the necessary protection that must be available at the time of communications and what related to it of privacy provisions to ensure confidentiality of communications (AlShamisi, 2023).

The rights of data subjects are a cornerstone of data protection regulations, and Article 5 of the Federal Decree Law No. 45/2021 on the Protection of Personal Data ensures that data processing is conducted fairly, transparently, and legitimately for specific and clear purposes. These provisions promote transparency and accountability while aligning with international data protection principles (Szalay, 2019).

This research highlights the shared fundamental principles between the UAE Data Protection Regulations and the GDPR in their approach to personal data processing. Both emphasize the importance of lawful, fair, and transparent data processing. Furthermore, they emphasize purpose limitation and data minimization to ensure data is used only for its intended purpose and that only necessary data is collected. Consent plays a pivotal role in data privacy (AlShamisi, 2023).

Both the UAE and the European Union (EU), through the GDPR, recognize the significance of consent in protecting individuals' rights in the processing of their personal data. Key similarities in their consent conditions include the right to withdraw consent, which must be easy and accessible to the data subject. In the context of data processing, obtaining consent is crucial. However, exceptions are necessary in certain situations. The UAE Data Protection Regulations and the GDPR provide provisions for lawful data processing without explicit consent, such as protecting the public interest, data becoming public through the data subject's actions, and fulfilling obligations in employment and social security (Thanvi, 2023).

The UAE Federal Decree Law No. 44 of 2021 established the Emirates Data Office, which plays a central role in data protection. The office formulates policies, strategies, and legislation in collaboration with competent authorities, supervises their implementation, and ensures compliance. It represents the UAE in regional and international forums, reinforcing the nation's commitment to global data protection standards (AlShamisi, 2023).

The protection of personal data in an era of rapidly advancing technology is of paramount importance. The rise of electronic data processing has presented both opportunities and challenges in safeguarding the privacy and rights of individuals. While numerous studies have explored data protection regulations and their implications, there exists a noticeable gap in the literature pertaining to a comparative analysis between the UAE data protection laws and the EU GDPR.

This research aims to bridge this gap by conducting a comprehensive examination of the legal frameworks in the UAE and the EU. By comparing these two regulatory environments, our study seeks to provide a deeper understanding of the commonalities and distinctions in their approach to personal data protection. We will delve into the definitions of personal data, the principles of data processing, consent requirements, exceptions, and the role of the Emirates Data Office, to shed light on how these two regions address the pressing issues related to data privacy.

This research is grounded in a theoretical framework that draws from the fields of data protection and privacy law. Central to this framework are the core principles of fairness, transparency, and accountability, which are fundamental to effective data protection regulations. Additionally, we rely on international data protection principles that guide the development and implementation of laws in this domain.

The relevance of this study cannot be overstated, given the global nature of data processing and the cross-border flow of personal information. In an interconnected world, individuals' data may traverse international boundaries, necessitating a harmonized approach to data protection. By comparing the UAE and EU data protection regulations, this research offers insights that are not only beneficial to policymakers and legal experts but also to organizations and individuals who operate in or interact with these regions (Younies & Al-Tawil, 2020). Understanding the similarities and differences in the legal frameworks can facilitate compliance and provide clarity on the rights and responsibilities of data subjects, controllers, and processors.

This paper is structured as follows. Section 2 provides an overview of the literature review. Section 3 is dedicated to detailing the research methodology employed. In Section 4, we highlight the principal results of the study. Following this, Section 5 delves into the main regulations concerning the protection of personal data, exploring both the provisions in the UAE Federal Law and the EU GDPR. Finally, Section 6 offers a comprehensive conclusion.

2. LITERATURE REVIEW

Several studies address the protection of personal data, as follows.

AlShamisi (2023) in her paper provides a comprehensive analysis of Federal Law No. 45 of 2021 concerning the protection of personal data in the UAE. By examining the scope of the law,

the conditions for processing personal data, and its adequacy in safeguarding privacy, this study contributes to the ongoing discussions surrounding data protection. It highlights the importance of robust legislation and effective implementation to ensure individuals' privacy rights are protected in the digital era.

Ducato (2020) aims to critically review the GDPR information requirements and national adaptations where the purpose of processing is scientific research. She pointed out that, due to the particularities of the legal system applicable to research situations, information regarding processing plays an important role for the data subject. However, this analysis shows that the information requirements or mandatory disclosures introduced by the GDPR are not entirely satisfactory and have some shortcomings.

Malgieri and De Hert (2020) highlight the substantial volumes of personal data processed in research endeavors. Many researchers, predominantly those in the field of information and communication technology (ICT), create algorithms that could have profound implications for individuals whose data is processed. The author underscores that while the GDPR does lay down specific guidelines and safeguards for the processing of personal data in research, there remains a degree of ambiguity and uncertainty. This is particularly noteworthy when considering the varying interpretations and implementations of GDPR at the national level.

Ali (2021) focuses on the GDPR. The study provides a comprehensive analysis of the GDPR as a legislative tool for protecting personal data in the context of its technical processing. Furthermore, a comparative analysis is conducted with French and Egyptian laws, as well as the Dubai International Financial Centre (DIFC) law, to highlight similarities and differences in their approaches to data protection.

Sethu (2020) emphasizes significance of cybersecurity is on the rise due to widespread and significant breaches in data security globally. Each day, nations encounter the trials posed by new security threats. Safeguarding the data of citizens and ensuring their privacy within that data is deemed a fundamental entitlement. Hence, it is crucial to stay abreast of legal advancements and regulations that demand heightened protection. This research scrutinizes the existing legislations in the EU, the U.S., India, and the UAE, examining the specific areas where each jurisdiction demonstrates exceptional proficiency in safeguarding data security concerns.

3. RESEARCH METHODOLOGY

The study will adopt the comparative analytical methodology. The comparative analytical method will be employed in this study to compare the UAE Federal Law No. 45 of 2021 related to the Protection of Personal Data and the European General Data Protection Regulation (GPDR No. 679 of 2016). This method involves a systematic examination of legal provisions, case law, and relevant documentation in both regions. The study will analyze key aspects such as the definition of personal data, data subject rights, consent requirements, data breach notification, cross-border data transfers, enforcement mechanisms, and penalties for non-compliance. By thoroughly examining these aspects, the research aims to provide a thorough insight into the parallels and distinctions between the UAE's data protection framework and the GDPR.

In the initial phase of preparing this paper, which began in early 2022, the authors diligently gathered a wealth of pertinent data and sources related to the subject at hand. This rigorous data collection effort included a wide array of highly significant primary legal sources, such as the UAE Federal Law No. 45 of 2021, the EU GDPR No. 679 of 2016, and other relevant information extracted from reputable websites. Our scholarly pursuit relies on two primary sources of authority. The first source comprises the relevant legal provisions outlined in the UAE Federal Law No. 45 of 2021 and the EU GDPR No. 679 of 2016. The second source involves a comprehensive examination of legal perspectives, encompassing case law and judicial decisions pertaining to the subject matter.

This meticulous data collection process has provided the authors with a substantial foundation of legal insights that substantially underpin the completion of this study. With the principal aim of advancing our comprehension of the study's objective or research question, our work has greatly benefited from these foundational concepts and ideas. They have paved the way for thorough analyses, ultimately yielding significant and academically valuable outcomes. We aspire to see these findings not only enrich scholarly discourse but also stimulate future research initiatives in this field.

Following the completion of data collection, the authors proceeded to analyze all relevant legal provisions acquired from previous legislation. This entailed a comprehensive review of the explanations and interpretations available for these legal provisions in various jurisprudential publications, encompassing both general and specialized sources. In essence, the authors have amassed a notable collection of key sources, including the UAE Federal Law No. 45 of 2021, the EU GDPR No. 679 of 2016, and data from websites. Thus, the information presented in this paper is drawn from two primary sources. The first includes the relevant legal provisions within the UAE Federal Law No. 45 of 2021 and the EU GDPR No. 679 of 2016. The second involves the analysis of diverse legal perspectives on the topic. This rigorous data collection process undeniably furnished the authors with an array of legal insights that have, in turn, contributed to the successful completion of this study. These insights and ideas have paved the way for the required comprehensive analyses, resulting in the emergence of several significant findings that will add substantial value to this paper and open new avenues for future research endeavors.

The case study method is an alternative method to study protection of personal data. This method involves an in-depth exploration of specific cases or scenarios related to data protection and privacy in the UAE and the EU. It could provide valuable insights into how these regulations are applied in real-world situations. However, it may lack the broader comparative perspective offered by the chosen methodology.

4. RESULTS

After finalizing the study and conducting an analysis of the subject, the research has yielded a series of key findings and outcomes. Specifically, these results pertain to the examination and comparison of the regulatory frameworks governing personal data protection in the UAE and the EU, the following results have transpired:

1) To safeguard user data, there must be fundamental principles and certain fair and equitable frameworks.

2) Users have the right to erase, commonly referred to as the "right to be forgotten". This right empowers users to request the deletion of their data at their discretion.

3) Users maintain the right to provide consent for data sharing, and they also possess the right to revoke this consent at any time, as per their wishes and requests.

4) The UAE office is the faithful guard of users' rights, which helps protect their basic rights.

5) The alignment between the UAE's definition and that of the GDPR underscores the UAE's commitment to upholding internationally recognized data protection standards and best practices, promoting legal consistency and harmonization.

5. DISCUSSION

5.1. Personal data definition

Generally, the definition of personal data plays a pivotal role in data protection law, shaping the extent of legal provisions' reach and application. It grants individuals authority over their personal information while imposing specific responsibilities on organizations to safeguard personal data against unauthorized access, utilization, or disclosure (Meshaal, 2017).

In the UAE, personal data definition aligns with international standards and best practices. Within the UAE's data protection legal framework, personal data encompasses: "any information about an identified or identifiable natural person, whether directly or indirectly identifiable through elements like their name, voice, identification number, electronic identifier, geographic location, or one or more physical, physiological, economic, cultural, or social attributes" (Federal Decree Law No. 45/2021 on the Protection of Personal Data, 2021, Article 1). This definition encompasses sensitive personal data and biometric data as well (AlShamisi, 2023).

It can be asserted that the EU has accumulated substantial expertise in data protection, dating back to the 1980s. Numerous countries worldwide have turned to the guidelines established by the EU's GDPR as a reference point when formulating their own data protection legislation (Hustinx, 2015).

The UAE's definition of personal data closely mirrors the definition provided in Article 4(1) of the GDPR (AlTohamy, 2018). According to the GDPR, "personal data" encompasses information that pertains to an identified or identifiable natural person. An identifiable natural person can be directly or indirectly recognized through various means, including but not limited to a name, identification number, location data, online identifier, or one or more characteristics specific to their physical, physiological, genetic, mental, economic, cultural, or social identity (European Parliament, the Council of the European Union, 2016, Article 4).

In UAE law, personal data is categorized into three types. The first category is *regular personal data*, which includes general and non-confidential information that does not disclose sensitive or personal details about an individual. This type encompasses data such as names, addresses, dates of birth, social statuses, and educational levels (AlShamisi, 2023).

This alignment between the UAE's definition and the GDPR's definition of personal data is significant for several reasons. It establishes a common terminology and understanding in the global context of data protection, facilitating international communication and cooperation on data privacy matters. Furthermore, it demonstrates the UAE's commitment to adhering to internationally recognized standards and best practices in data protection, fostering legal consistency and harmonization (AlMarzooqi et al., 2020).

The classification of personal data into regular and sensitive categories in UAE law highlights the importance of categorizing data based on its sensitivity. This classification guides organizations in applying appropriate levels of protection and security measures to different data types. It also underscores the UAE's intent to balance data utility for legitimate purposes with safeguarding individuals' privacy rights (Ghandour & Woodford, 2019).

For organizations operating in the UAE, especially those with international connections, awareness of this alignment is crucial. It implies the need to adopt data protection measures and practices that align with GDPR standards to ensure compliance with UAE law. Ultimately, the alignment serves as a framework for consistent and responsible data handling practices in the UAE, facilitating international data flows and enhancing privacy protection for individuals in the country (El-Gheriani, & Hashish, 2023).

The second category is *sensitive personal data* that is "any data that directly or indirectly reveal a natural person`s racial or ethnic origin, political opinions, philosophical beliefs, religious beliefs, family background, criminal record, biometric measurements, or any data relating to the person's physical, mental, genetic, or sexual health, including information regarding the provision of healthcare services that disclose their health status" (Federal Decree Law No. 45/2021 on the Protection of Personal Data, 2021, Article 1). The third category is *biometric personal data*; this category includes information obtained from certain technologies related to an individual's physical or physiological characteristics. Examples of biometric personal data include facial images, fingerprint data, or other information used for unique identification (Federal Decree Law No. 45/2021 on the Protection of Personal Data, 2021, Article 1).

5.2. Rights of the data subject

The data subject's rights are safeguarded by the data protection regulations in the UAE. Article 5 of the Decree-Law outlines a series of provisions to ensure that data processing is conducted appropriately. This includes processing data fairly,

transparently, and legitimately, and gathering personal data for specific and clearly defined purposes. The article also establishes a condition that prohibits data from being processed at a later time in a way that is inconsistent with the originally specified purpose (Federal Decree Law No. 45/2021 on the Protection of Personal Data, 2021, Article 1).

From a regulatory standpoint, these provisions are essential for safeguarding individuals' data privacy rights. They promote transparency, accountability, and responsible data handling practices, aligning with international data protection principles (Ellamey, & Elwakad 2023).

The UAE Data Protection Regulations (Federal Decree Law No. 45/2021 on the Protection of Personal Data, 2021, Article 5), and the GDPR share several fundamental principles in their approach to personal data processing. These principles are vital for establishing robust data protection frameworks, even though there may be variations in the depth and clarity with which each regulation addresses them:

Lawfulness, fairness, and transparency: Both the UAE Data Protection Regulations and GDPR emphasize that personal data processing must be conducted in a lawful, fair, and transparent manner. This commonality underscores the importance of adhering to ethical and legal standards when handling personal data. However, GDPR provides more detailed guidance on this principle.

Purpose limitation: The principle of purpose limitation is central to both regulations. UAE Data Protection Regulations stress that personal data should be collected for specific and clear purposes and should not be handled in a way that is inconsistent with its intended purposes unless it is similar or closely related. GDPR articulates this principle with greater specificity, including exceptions for archiving, scientific research, and statistical purposes.

Data minimization: Both regulations acknowledge the importance of data minimization, ensuring that personal data is adequate, relevant, and limited to what is necessary for the intended purposes. This principle aligns with the concept of collecting only the data that is strictly required for the intended use.

Accuracy and updates: Both regulations emphasize the accuracy of personal data. UAE Data Protection Regulations require that data must be accurate, correct, and updated as needed, with mechanisms in place for correction. GDPR similarly mandates data accuracy and includes provisions for prompt correction of inaccuracies.

Storage limitation: Both regulations recognize the importance of limiting the retention of personal data. UAE Data Protection Regulations state that personal data should not be kept after fulfilling the processing purpose unless anonymized. GDPR elaborates on this principle, emphasizing that personal data should not be retained for longer than necessary for the purposes for which it is processed.

Integrity and confidentiality: Both regulations underscore the necessity of maintaining the integrity and confidentiality of personal data. They mandate the implementation of suitable technical and organizational measures to safeguard against unauthorized or unlawful processing, as well as to prevent accidental loss, destruction, or damage. This principle ensures data security and confidentiality.

5.3. Conditions necessary for the consent on the usage of those data

The origin is that a list of the rights of users must be included — those rights that must be present by law, and these rights are given in the next subsections.

5.3.1. Consent of the data subject

In our data-driven world, protecting personal information has become paramount. Both the UAE and the EU, through its GDPR, recognize the pivotal role of consent in ensuring the privacy and rights of individuals in the processing of their personal data. This shared emphasis reflects a commitment to safeguarding individuals' autonomy over their data and underscores the global significance of this fundamental principle (AlTohamy, 2018).

According to Article 6 of Federal Decree Law No. 45 of 2021, the entity responsible for managing users' data is required to substantiate the user's consent when dealing with their data. This initial point in Article 6 mandates that the data controller must have the capacity to prove the consent granted by the data subject, and this is also what Article 7 of the GDPR stipulates "where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data" (European Parliament, the Council of the European Union, 2016, Article 7).

The Decree-Law in Article 6 demands — the second point — that the consent that the user gives to the controller — is prepared in an easy, simple, unambiguous, and easy-to-reach manner — and whatever the approval is, whether in a written or electronic way (Federal Decree Law No. 45/2021 on the Protection of Personal Data, 2021, Article 5). Article 7 of the GDPR emphasized these previous conditions but added that any deducted part of that consent is considered a violation of users' rights and is not binding at all. It was stated in the second point of Article 7 that:

"If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding" (European Parliament, the Council of the European Union, 2016, Article 7).

When we analyze the consent conditions outlined in Article 6 of Federal Decree Law No. 45 of 2021 of UAE Data Protection Regulations and Article 7 of GDPR, several key similarities emerge.

Similar emphasis on consent: Both the UAE Data Protection Regulations and the GDPR place a similar and strong emphasis on the significance of consent in the context of personal data processing. This shared emphasis demonstrates a commitment to internationally recognized data protection standards and reflects their dedication to protecting individuals' data rights (AlTohamy, 2018).

Demonstrating consent: One commonality between the UAE Data Protection Regulations and GDPR is the requirement for Entities responsible for data management to prove that data subjects have granted consent for the processing of their personal

data. This aligns with the principles of accountability and transparency, emphasizing the importance of clearly establishing consent as the foundation of lawful data processing practices (Ali, 2021).

Clarity and accessibility of consent: Both regulations stress the need for clarity and accessibility when obtaining consent. In the UAE, consent should be provided in a clear, simple, and easily accessible manner, whether in writing or electronically. GDPR echoes this sentiment, emphasizing that consent requests should be presented in a comprehensible and readily accessible form, using plain and clear language. This shared commitment ensures that individuals can provide informed consent without any ambiguity or confusion (AlShamisi, 2023).

5.3.2. Right to withdraw consent

It must be written in an obvious way that the user has the right to withdraw consent from the consent, and the procedures for revert must be easy and accessible to the user — this is stipulated in paragraph C of the first point of Article 6. Also, the data subject may revert his consent at any time. And this does not affect the legality and legitimacy of the processing based on the consent that was given before the revert (the second point of Article 6) (Meshaal, 2017).

For the GDPR: "The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent" (European Parliament, the Council of the European Union, Article 7, p. 37, 2016). The GDPR establishes several key principles regarding consent:

Right to withdraw consent: Under the GDPR, data subjects have the unequivocal right to withdraw their consent at any time (there is no specific method or deadline mentioned for the withdrawal of consent). This withdrawal does not retroactively affect the lawfulness of processing that relied on consent before its withdrawal.

Ease of withdrawal: The GDPR places great importance on making the withdrawal process as simple as granting consent. Data subjects should not encounter undue obstacles when choosing to withdraw their consent.

Freely given consent: GDPR emphasizes that consent must be freely given. This means that data subjects should not face coercion or pressure when deciding whether to grant or withhold their consent. Specifically, the GDPR highlights the importance of assessing situations where the performance of a contract or service depends on consent for the processing of personal data that is not strictly necessary for fulfilling that contract (Meshaal, 2017).

5.4. Cases of processing personal data without the consent of the subject

Data protection regulations are essential for safeguarding individuals' privacy and ensuring the responsible handling of personal data. In the context of data processing, obtaining consent from the data subject is a fundamental requirement. However, there are situations where data processing without explicit consent becomes necessary (Sweeney, 2011).

The UAE Data Protection Regulations and the GDPR have provisions that allow certain exceptions to the general prohibition of processing personal data without the consent of the data subject. In the UAE, Article 4 of Federal Decree Law No. 45 of 2021 outlines several scenarios where processing without consent is considered lawful. These include cases where processing is necessary to protect the public interest, instances where data becomes public through the data subject's actions, and situations related to legal proceedings, occupational medicine, public health, archival purposes, protecting the data subject's interests, and fulfilling obligati1ons in employment and social security (Federal Decree Law No. 45/2021 on the Protection of Personal Data, 2021, Article 4).

On the other hand, the GDPR, in Article 9, strictly prohibits the processing of special categories of personal data without explicit consent. However, it provides exceptions in certain cases. These exceptions include situations where the data subject gives explicit consent for specific purposes, processing is necessary for employment and social security obligations, protection of vital interests, processing by not-for-profit organizations, publicly shared data, legal claims, substantial public interest, preventive or occupational medicine, public health, and archiving, scientific research, historical research, or statistical purposes based on Union or Member State law.

Both the UAE Data Protection Regulations and the GDPR acknowledge the importance of consent as a fundamental principle for processing personal data. However, they differ in their approach to exceptions. The UAE regulations provide a comprehensive list of scenarios where data processing without consent is permissible, focusing on public interest, legal proceedings, and various aspects of healthcare and research. This approach allows for flexibility and adaptability in different contexts. In contrast, the GDPR takes a more restrictive stance by prohibiting the processing of special categories of personal data without explicit consent, with only limited exceptions. These exceptions are strictly defined, emphasizing the need for proportionality, protection of fundamental rights, and adherence to Union or Member State laws.

Furthermore, one of the cases that are excluded where the processing of personal data is lawful despite the lack of consent of the data subject is when "the processing is necessary for occupational or preventive medicine to assess the ability of employees to work, medical diagnosis, or provide health care, medicines, drugs, and medical devices, according to the legislation in force in the country" (Federal Decree Law No. 45 of 2021 on the Protection of Personal Data, 2021, Article 4/4). And "that the treatment is necessary for public health purposes and includes protection from communicable diseases and epidemics or to ensure the safety and quality of health and international care, medicines, drugs, and medical devices" (Federal Decree Law No. 45/2021 on the Protection of Personal Data, 2021, Article 4/5).

5.5. Establishment of the UAE Data Office

The UAE Federal Decree Law No. 44 of 2021 established the UAE Data Office. Article 2 of this law provided that "the Data Office is affiliated with the Council of Ministers and holds legal personality, financial and administrative independence, and legal capacity to undertake the business and actions necessary to implement its competencies".

The Emirates Data Office, established under a Decree Law, holds a multitude of vital responsibilities in the realm of data protection:

Policy and legislation: Firstly, the office plays a pivotal role in formulating policies, strategies, and legislation pertinent to data protection. This endeavor is undertaken in close collaboration with competent authorities, with subsequent supervision of policy and law implementation following approval by the Council of Ministers.

Monitoring and standards: The office is tasked with proposing and endorsing the foundational principles and standards essential for monitoring the application of federal legislation governing data protection. This activity, too, is carried out in coordination with relevant competent authorities.

Complaints and grievances: Another significant responsibility is the development and approval of comprehensive systems for managing complaints and grievances tied to data protection matters. These systems are established in collaboration with competent authorities to ensure effective redressal mechanisms. The office will implement control operations on the application of federal legislation governing data protection, conduct the necessary investigations to ensure the extent of compliance with it, and spread awareness regarding the provisions and requirements of the law by organizing conferences, seminars, workshops, and others.

Guides and instructions: The office is further mandated to issue comprehensive guides and instructions that serve as practical tools for the implementation of data protection legislation, facilitating compliance across various sectors.

In the event of violations, the data subject can submit a complaint to the office that investigates it, as stipulated in Article 24 of Federal Decree Law No. 45 of 2021. In case the violation is proven, the office will impose administrative penalties in accordance with Article 26 of Federal Decree Law No. 45 of 2021, which states that "the Council of Ministers shall issue a decision to specify the acts that constitute a violation of the provisions of this Decree-Law, its executive regulations, and the administrative penalties to be imposed".

It is right to say that the UAE office is the faithful guard of users' rights that helps protect fundamental rights. But the office's role also includes the ability to represent users and present cases more clearly, since the European Union and member states have had laws to protect data for more than 35 years. Despite this, some small companies there ignored paying relatively low fines (up to 150,000 euros) to users whose rights were violated.

6. CONCLUSION

The drafting of a data protection law is a matter of great importance, especially since the UAE government has been keen to protect its users' data and its keenness to protect the right to privacy, especially as these technological matters are always evolving. When the law is established and implemented, it is for the present and the future. Therefore, the legislative and executive authorities must constantly review this law and work to update it, address any potential problems, provide more clarity, and compel governmental and non-governmental organizations working in the state to comply with the law to protect users and protect the right to their privacy. Striking the required balance between those rights and the right to circulate information and the right to expression. And here are a set of results and recommendations we came through this research.

Firstly, the UAE's definition of personal data closely with international standards and best practices, particularly the EU GDPR. Personal data encompasses a wide range of identifying elements and attributes that pertain to an individual who can be identified or is already identified.

Secondly, the UAE's data protection regulations emphasize the rights of data subjects. These rights include the fair, transparent, and lawful processing of personal data, as well as the collection of data for specific and legitimate purposes. The data subjects also have the right to access, modify, and delete their personal information, and the data must be processed securely to ensure integrity and confidentiality.

However, there are certain areas where the UAE's data protection laws can be improved. The purpose limitation principle, which restricts further processing of personal data for purposes other than the initial ones, should be clearly defined in the legislation. Additionally, the concept of consent should be further developed, specifying the conditions and procedures for obtaining and revoking consent in a clear and accessible manner.

Furthermore, the discussion points out that there are exceptions to processing personal data without the consent of the subject in cases of public interest or for occupational and preventive medicine purposes. While these exceptions are necessary, they should be subject to judicial oversight to protect the rights and interests of data subjects.

To ensure the effective implementation and enforcement of data protection laws, the UAE has established the UAE Data Office as an independent authority with the power to enforce regulations, conduct investigations, and impose penalties on entities that violate data protection laws. This authority plays a crucial role in safeguarding personal data and ensuring compliance with data protection regulations.

This research primarily focuses on comparing the UAE Data Protection Regulations with the GDPR. While this comparison offers valuable insights, it may not encompass the full spectrum of global data protection frameworks.

Firstly, scope of comparative analysis: This research primarily centers on the comparative analysis between the UAE Data Protection Regulations and the GDPR. As a result, its findings may not encompass the full breadth of data protection regulations globally.

Secondly, legal-centric analysis: The analysis is predominantly grounded in a legal perspective, concentrating on the examination of textual congruities and disparities within the regulations. Consequently, it may not encompass the broader practical and societal implications of these regulations. Thirdly, by presenting several significant results, this study lays the groundwork for prospective research in the same field.

This research underscores the importance of ongoing monitoring, evaluation, and adaptation of data protection laws in response to technological advancements and evolving privacy concerns. Future research endeavors in this field should focus on assessing the practical implementation of these regulations, exploring user experiences and challenges, and further refining legal provisions to strike an optimal balance between individual privacy rights and the free flow of information. Additionally, international comparisons and case studies can provide valuable insights into global data protection practices and their impact on society.

REFERENCES

1. Ali, M. H. A. (2021). The legal system for protecting processing personal data electronically: A comparative analytical study under the European regulations and relevant legislation. *Journal of Legal Sciences, Ajman University (UAE), 7*(14), 73–118. https://www.ajman.ac.ae/upload/files/law/JLS_issue_14.pdf
2. AlMarzooqi, F. M., Moonesar, I. A., & AlQutob, R. (2020). Healthcare professional and user perceptions of eHealth data and record privacy in Dubai. *Information, 11*(9), Article 415. https://doi.org/10.3390/info11090415
3. AlShamisi, H. (2023). The protection of personal data in light of Federal Law No. 45 of 2021: A comparative study. *Security & Law Journal, Dubai Police College, 31*(1), 9–54. http://search.mandumah.com/Record/1345083
4. AlTohamy, S. (2018). Nitaq alhimayat alqanuniat lilbayanat alshakhsiat walmaswuwliat altaqsiriat ean muealajatiha (dirasat fi Alqanun Al'iimarati) [The scope of legal protection for personal data and liability for its processing (A study in Emirati law)]. *Journal of Legal and Economic Research, 8*(66), 615–668. https://doi.org/10.21608/mjle.2018.156150
5. Ducato, R. (2020). Data protection, scientific research, and the role of information. *Computer Law & Security Review, 37*, Article 105412. https://doi.org/10.1016/j.clsr.2020.105412
6. European Parliament, the 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, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union.* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
7. El-Gheriani, M., & Hashish, A. (2023). Egypt amends its competition law to establish a pre-merger control system. *Journal of European Competition Law & Practice, 14*(2), 106–112. https://doi.org/10.1093/jeclap/lpad014
8. Ellamey, Y., & Elwakad, A. (2023). The criminal responsibility of artificial intelligence systems: A prospective analytical study. *Corporate Law & Governance Review, 5*(1), 92–100. https://doi.org/10.22495/clgrv5i1p8
9. Federal Decree Law. No. 44/2021. (2021). United Arab Emirates Ministry of Justice. https://www.dha.gov.ae/uploads/082022/Federal%20Decree%20Law%20No2022823792.pdf
10. Federal Decree Law No. 45/2021 on the Protection of Personal Data. (2021). Dubai Judicial Institute. https://u.ae/-/media/Documents-2023/ArFederal-Decree-Law-No-45-of-2021-regarding-the-Protection-of-Personal-Data.pdf
11. Ghandour, A., & Woodford, B. J. (2019). Ethical issues in artificial intelligence in UAE. In *2019 International Arab Conference on Information Technology (ACIT)* (pp. 262–266). IEEE. https://doi.org/10.1109/ACIT47987.2019.8990997
12. Hustinx, P. (2015). *EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation.* https://edps.europa.eu/sites/edp/files/publication/14-09-15_article_eui_en.pdf
13. Malgieri, G., & De Hert, P. (Eds.). (2020). Legal and ethical challenges of data processing in the research field [Special issue]. *Computer Law & Security Review, 37*. https://www.sciencedirect.com/journal/computer-law-and-security-review/special-issue/10S60T5Q4Z8
14. Meshaal, M (2017). Alhaqu fi mahw albayanat alshakhsiat dirasat tahliliat fi daw' layihat himayat albayanat bial'iitihad al'uwrubiyi GDPR wa'ahkam almahakm al'uwrubiya [The right to erasure of personal data: An analytical study in light of the European Union's General Data Protection Regulation (GDPR) and European Court Rulings]. *Majala Aldirasat Alqanuniat Waliaqtisadia, 3*(2), Article 2. https://doi.org/10.21608/jdl.2017.102564
15. Sethu, S. G. (2020). Legal protection for data security: A comparative analysis of the laws and regulations of European Union, US, India and UAE. In *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)* (pp. 1–5). IEEE. https://doi.org/10.1109/ICCCNT49239.2020.9225488
16. Sweeney, L. (2011). [Comments from Latanya Sweeney and the Data Privacy Lab to the Department of Health and Human Services, Office of the Secretary, and Food and Drug Administration]. Retrieved from https://dataprivacylab.org/projects/irb/DataPrivacyLab.pdf?yui_3_18_1_1_1478271873015_2412=1
17. Szalay, G. (2019). The impact of the lack of transparency on corporate governance: A practical example. *Corporate Law & Governance Review, 1*(2), 21–28. https://doi.org/10.22495/clgrv1i2p2
18. Thanvi, I. A. (2023). Challenges in implementation of Personal Data Protection Law No. 45 of 2021: A case study of the United Arab Emirates. *Cyber Law Reporter, 2*(3), 1–15. https://thelawbrigade.com/wp-content/uploads/2023/07/Irfan-Ali-Thanvi-CYLR.pdf
19. Younies, H., & Al-Tawil, T. N. E. (2020). Effect of cybercrime laws on protecting citizens and businesses in the United Arab Emirates (UAE). *Journal of Financial Crime, 27*(4), 1089–1105. https://doi.org/10.1108/JFC-04-2020-0055