EDITORIAL

Data Protection in the United Arab Emirates

Welcome to this special issue of the Global Privacy Law Review (GPLR), focussed on the vibrant and evolving legal environment of the United Arab Emirates (UAE). As the UAE continues to assert its position as a leading financial and legal hub in the Middle East, understanding its legal nuances has never been more crucial for academics, practitioners, and global businesses alike.

The UAE's legal system is unique, blending civil law structures with elements of Islamic law, all while rapidly adapting to the demands of a burgeoning international commercial market. Recent reforms in areas such as arbitration, commercial transparency, and technological innovation, reflect the UAE's commitment to fostering a legal environment that supports growth and fairness.

This issue arrives at a particularly pivotal time, as the UAE is taking significant strides in enhancing data protection and privacy laws and aligning itself with global standards. The introduction of Federal Decree-Law No. 45 of 2021 (UAE Data Protection Law) marks the UAE's first comprehensive federal data protection legislation. Coupled with the establishment of the UAE Data Office, these developments underscore a robust commitment to safeguarding personal data. Furthermore, the updates in data protection regulations by the Dubai International Financial Centre (DIFC) and Abu Dhabi Global Market (ADGM) enhance the legal framework, ensuring stringent protections that echo rigorous international standards like the EU's General Data Protection Regulation (GDPR).

This special issue aims to provide a comprehensive insight into these developments, offering a platform for experts from various legal spheres to share their research, analysis, and opinions. The articles featured range from in-depth analysis of recent legislative developments to explorations of regulatory changes and their implications for both local and international stakeholders.

We are profoundly grateful to Mr Jacques Visser, the Commissioner of the Data Protection Authority in DIFC, for graciously providing the foreword for this special issue on the UAE. His insightful contribution not only elevates the discourse within these pages but also provides our readers with a nuanced understanding of the significance of data protection laws in a rapidly evolving legal and technological landscape. Thank you for your pivotal role in enriching this publication and for your ongoing efforts to safeguard personal data within the DIFC.

We are also grateful to the multitude of contributors who have enriched this issue with their expertise.

First, in our *articles* section, Mustafa Alnujaifi, Mohammad Noaman Atallah, Noaman Atallah Alheety, Ziad Al-Enizi and Ramzi Madi examine the regulatory framework governing the right to information in the UAE.[1]

The authors argue that this right is fundamental in equipping individuals with the necessary awareness to participate effectively in public affairs. The article delves into this right under three primary dimensions: (1) understanding the associated terms and restrictions, (2) identifying the confines placed on the freedom to obtain information, and (3) outlining the critical conditions necessary to exercise this right. The article calls for an amendment to existing guidelines to distinguish between ordinary circumstances and extraordinary instances where the need for information arises.

The article stresses the significance of protecting personal privacy, positing it as one of the primary exceptions to the free access and dissemination of information. It underlines the duty to safeguard information that bears relevance to an individual's private life, including elements such as one's dignity, family life and place of residence. This responsibility stems from a right to privacy. The authors also highlight governmental obligations to uphold the inviolability of one's dwelling, the privacy of one's correspondence, and each individual's intrinsic right to dignity – directives which are ingrained in various constitutions.

Moreover, the authors explore the boundaries of disclosing information. The article puts forth that without specific restrictions, the right to access information could negatively impact other essential rights. The authors propose a three-section test to strike a balance between

Notes

[1] Mustafa Alnujaifi, Mohammad Noaman Atallah, Noaman Atallah Alheety, Ziad Al-Enizi & Ramzi Madi, *Regulatory Framework Governing the Right to Information in the United Arab Emirates: An Analytical Examination*, in this issue at 99 (2024).

withholding and disclosing information. Public authorities can refuse the disclosure of specific information only if it aligns with this test. Additionally, the article acknowledges that high costs associated with obtaining information could deter individuals from exercising this right.

In their conclusion, the authors acknowledge that while currently there is no central authority tasked with issuing information in the UAE, the necessary data resides within disparate government bodies. The article suggests that the legislation enacted by the ruling authority determines the body from which information may be retrieved. The research also positions the protection of an individual's privacy and the right to access information as dual goals, both aimed at protecting individuals from intrusive state authorities.

In the second article, Ali Hadi Al Obeidi, Zeyad Jaffal and Jamal Barafi explore the concept of the *right to be forgotten* within the context of social media and the legal prerequisites necessary for its establishment, focusing specifically on the regulations in the UAE.[2]

The right to be forgotten, which comes within the scope of personal data rights, is the entitlement of individuals to request that their personal data is deleted when it no longer serves its original purpose.

The authors note that, in recognition of the importance of safeguarding personal data, the UAE government introduced the UAE Data Protection Law in 2021. This law underscores that personal data should not be kept after fulfilling the purpose of processing and can be retained only if the subject's identity is anonymized.

The article scrutinizes and assesses the conditions and restrictions for utilizing the right to be forgotten within social media platforms. The providers of these platforms must decide between erasing personal data and retaining it, while ensuring the individual remains anonymous. However, the authors argue that the right to retain anonymous data should not be automatically given to social network service providers but granted selectively, based on specific justifications established by the law.

The authors also reveal concerns over certain vague terms such as 'public interest' in the law that might compromise an individual's right to be forgotten. The UAE Personal Data Protection Law outlines certain exceptions where the individual has no right to request the erasure of their personal data; the authors argue that these exceptions should only apply when data deletion will contravene the law, emphasizing that the 'public interest' condition should be removed.

In conclusion, the article demonstrates that the right to be forgotten plays a significant role in the broader framework of the right to privacy in the UAE. The authors conclude that the right to be forgotten allows individuals to control their personal data, asking social media platforms to delete their information once it no longer serves its intended use. Furthermore, they note that further steps should be taken to provide clearer guidelines and conditions around the 'right to be forgotten' and 'public interest', to balance individuals' rights to privacy with the need to preserve public interest.

In the third article, Tariq Kameel, Ghaleb A. Elrefae and Reham Mahmoud Abumwais examine the role of Emirati lawmakers in securing the privacy of electronically processed personal health data.[3] Personal health data is sensitive information that should be safeguarded against unauthorized access or misuse. The authors note that, in the UAE, legislation has been devised to establish guidelines for the utilization of information and communication technology (ICT) in health sectors, including data collection and electronic storage, with the aim of ensuring optimal ICT usage in accordance with international standards.

Confidentiality of patient data is held in high regard, and any party that handles patient information is mandated to preserve the secrecy of this information. Consent is required to access or use the health data, with exceptions only made in circumstances authorized by law. This consent must be in writing; in cases involving unconscious patients or minors, their legal representative can provide this written consent. However, in certain circumstances provided for by Emirati legislators, the patient's consent can be overridden.

Emirati lawmakers' focus on personal health data regulation resonates with the goal of fostering sustainable development in the UAE. This is achieved by creating secure digital societies where individuals can live healthy and active lives, and by implementing fair, innovative healthcare services that match international standards. The onus is on health authorities in the country to cultivate a culture of personal health data protection and to increase public and institutional awareness about adhering to the stipulated protection measures.

In the fourth article, Bashar Talal Momani, Mohamed Ettoudar, Nour Alhajaya and Mahmoud Fayyad emphasize the essential nature of securing personal data privacy in the modern technological era, where virtual environments are teeming with both lawful and unlawful activities.[4] As a result of the ubiquitous use of smart technologies,

Notes

[2] Ali Hadi Al Obeidi, Zeyad Jaffal & Jamal Barafi, *Conditions for Exercising the 'Right to Be Forgotten' on Social Media under the 2021 UAE Data Protection Law*, in this issue at 109 (2024).

[3] Tariq Kameel, Ghaleb A. Elrefae & Reham Mahmoud Abumwais, *Electronically Processed Personal Health Data Privacy Protection in the UAE: An Analytical Study*, in this issue at 119 (2024).

[4] Bashar Talal Momani, Mohamed Ettoudar, Nour Alhajaya & Mahmoud Fayyad, *Securing Privacy: Safeguarding Against Cyber Threats in the UAE and Morocco*, in this issue at 126 (2024).

individuals often entrust large amounts of personal information to digital databases, including biometrics, health and medical records, and even current location data. The way these data are protected from cyber threats is critical, and the article underlines the need for a balance between protecting privacy and promoting free speech, whilst setting robust privacy controls for data confidentiality.

The article addresses relevant legislation in the UAE and Morocco as case examples. In Morocco, the requirement for explicit consent from individuals to process their personal data was established by Law No. 09.08 of 2009. The UAE's response to privacy concerns is discussed with the enactment of the UAE Data Protection Law alongside Federal Decree-Law No. 34 of 2021 on combating rumours and cybercrimes.

The authors conclude with the assertion that the right to privacy is fundamental, and current legislative efforts strive to heighten its protection, especially amidst advancements in personal rights. Cybersecurity laws aim to safeguard the privacy of internet users across all demographics, highlighting the importance of protecting electronic services from threats. The authors emphasize that legislative bodies still face significant challenges, particularly with the public's indiscriminate sharing of personal information and the low level of awareness regarding potential cybersecurity vulnerabilities.

In our *Report* section, Ramzi Madi from the Al Ain University in the UAE explores the application and regulation of DNA fingerprinting and its database in the UAE, following the implementation of Federal Decree by Law No. (39) of 2023.[5]

Madi argues that DNA fingerprinting represents a pivotal advance in forensic science, and its significance has been recognized in the UAE with a law specifically pertaining to this technology. He notes that the Federal UAE DNA Fingerprinting Database was brought into effect as of 1 November 2023 aiming to manage and regulate the database for various practical applications.

The UAE Ministry of Interior is primarily responsible for setting up and managing this Federal DNA Fingerprinting Database. The author argues that the database is used for multiple purposes, such as investigating crimes, identifying victims in crises, disasters, and accidents, and ascertaining the identity of unidentified bodies or missing persons. Various sources, like crime scene suspects, victims, found missing persons, and even employees exposed to danger due to their work, can provide biological samples for DNA fingerprinting. The law further lays down the methods and safeguards for preserving and managing these biological samples and rules governing their retention period.

Madi notes that the law also stipulates legal safeguards to protect the DNA fingerprint databases. Confidentiality of DNA fingerprinting data is emphasized, and any disclosure is prohibited unless stipulated by law. Penalties, including temporary imprisonment and financial fines, can be applied for misuse of the database. The UAE presents this law as part of its commitment to harnessing advancements in forensic science and pioneering a new era of regulation and governance surrounding DNA fingerprinting while maintaining strict legal and ethical standards.

I would like to acknowledge and express my gratitude for the fantastic work carried out by Ramzi Madi in this issue, not only for his excellent contributions, but also for proposing and coordinating the work of the other authors. This issue would not have been possible without his help.

Finally, in the *News* column, Nick Roudev of Linklaters put together and edited Middle East Privacy News, which tracks significant developments in some of the key countries in the region in the area of data protection, privacy and cybersecurity.[6]

The authors who participated in this piece are Sharif Shihata (*Shalakany Law Office*) from Cairo, Egypt; Eyal Roy Sage (*AYR Lawyers*) from Bnei Brak, Israel; Nick Roudev (*Linklaters*) from Dubai, UAE; and Burak Ozdagistanli, Sümeyye Uçar and Begüm Alara Sahinkaya (*Ozdagistanli Ekici*) from Istanbul, Turkey.

This news column provides concise reports to keep the reader up to date with some of the most recent developments in the Middle East region.

As you delve into the articles, report and news sections, we encourage you to reflect on the complexities and innovations of the UAE legal system. It is our hope that the discussions, analysis, and perspectives offered here not only inform but also inspire continued excellence and innovation in the practice of data protection.

In closing, may this special issue serve as a valuable resource and resonate beyond its pages, influencing policy, practice, and the protection of privacy rights in the UAE and beyond. We look forward to your feedback and to fostering ongoing discussions on these vital legal issues.

Sincerely
Ceyhun Necati Pehlivan
Editor-in-Chief

Notes

[5] Ramzi Madi, *Establishment of a DNA Fingerprinting Database in the UAE*, in this issue at 133 (2024).

[6] *Middle East Privacy News* (Nick Roudev ed.) in this issue at 136 (2024).