EDITORIAL

Foreword

In this edition of the Global Privacy Law Review (GPLR), the contributors address a variety of interesting and relevant topics for privacy practitioners in the Middle East and beyond, inter alia: (1) analysing the regulatory framework governing the right to information in the United Arab Emirates (UAE), focussing on its requirements, restrictions, and the conditions necessary for exercising this right; (2) a very insightful study into the 'right to be forgotten', its origins and the legal prerequisites necessary to assert this right within the ambit of social media platforms, and the conditions for its substantiation under the UAE Personal Data Protection Law; (3) examining the role of Emirati lawmakers in securing the privacy of electronically processed personal health data; (4) evaluating, on a comparative basis, the effectiveness of legal frameworks in the UAE and Morocco concerning cybersecurity risks and safeguarding the privacy of individuals in the digital world in that context with some key recommendations; (5) the establishment and regulation of a federal DNA fingerprinting database in the UAE, marking a significant advancement in the UAE's forensic science capabilities and the consequences thereof also from a legal perspective; and (6) considering the evolution and current state of data protection regulatory regimes in various Arab countries, focussing on their efforts to adapt to the needs of the digital economy and ensure consumer trust in digital trade and e-commerce.

The research and efforts that went into publishing these articles are crucial for advancing our knowledge and understanding of the complex issues often facing us as privacy practitioners and data protection regulators, and should be encouraged and commended.

One such complex issue currently facing us is the dynamic and often contentious topic of data sharing. Data has moved well beyond the notion of being the 'new oil' lubricating the wheels of a borderless digital economy. With artificial intelligence (AI) increasingly playing a pivotal role in personal data analytics, extracting insights and driving efficiencies across a global marketplace – data, and specifically personal data, is transitioning from 'new oil' to 'digital asset' in the form of the value of our personal data (in the form of our movements, preferences, spending habits etc.) represent to data aggregators and the like in the context of a Web 3.0 economy. This construct of monetizing personal data, as opposed to be solely focused on protecting it, has the potential to be powerful on an exponential level.

The dialogue between privacy professionals, regulators, governments and entities engaged in cross-border data transfers is often underpinned by a complex interplay of legal standards, regulatory requirements, cultural norms, and compliance attitudes. It is here where we often encounter the intricate concept of the 'adequacy' of a particular jurisdiction, which is intended to assess the protective measures and legal framework where an importer resides to understand to what extent individuals' personal data is protected from a basic human right and rule of law perspective.

In our experience, these discussions often centre around the pivotal role of government access to imported personal data and the protections and accountability inherent in the system to safeguard the rights of individuals in those circumstances. It is also here where the specific carve-outs in data protection laws allowing for government access to data under the guise of state security, law enforcement or crime prevention (often bypassing the awareness of the affected individuals) becomes a key area of focus.

The backdrop of our own experience in this context was the relatively recent adequacy assessment undertaken by the United Kingdom of the Dubai International Financial Centre's (DIFC's) data protection regime with the aim to establish a 'data bridge' between the two jurisdictions. As expected, such reviews are influenced significantly by evolving case law and the ongoing debate about the role of a so-called 'functioning democracy' in ensuring individual rights and offering redress where governments require access to personal data.

However, this topic has become much more nuanced in recent times. As the Economist Intelligence Unit's Democracy Index 2023 has shown, there appears to be a shifting metric of global governance structures and the findings question the relevance of democracy as an effective metric for data protection, and consequently considers the necessity of evaluating the rule of law independently from political systems.[1]

Notes

[1] Economist Intelligence Unit, *Democracy Index 2023* (2023), www.eiu.com/n/campaigns/democracy-index-2023 (accessed 29 May 2024).

This is understandably a very relevant consideration in regions like the Gulf Cooperation Council (GCC) and elsewhere, where political frameworks diverge markedly from the traditional western understanding of democracy. In places like the DIFC –where we can rely on advantages such as (1) governmental, statutory, regulatory and judicial independence and efficacy ensuring the rule of law; (2) the ambition to lead the debate in global best practice (also aspiring to clear standards and certification regimes in respect thereof); and (3) the drive to excel in a very competitive global marketplace– we know that such a system can serve as a pragmatic replacement for principles and protections that others may have associated with traditional democratic values, and the entrenchment of the rule of law therein, in the past.

This edition encourages a re-evaluation of the traditional assumptions in this context, advocating for a clear distinction between a political dispensation and the robustness of legal systems, where it concerns data protection. It also highlights, for example, the stringent due diligence and risk assessment requirements for data transfers in our DIFC Data Protection Law, particularly where government authorities are involved. These measures are crucial in balancing the 'obligation' to transfer personal data for the purposes of responding to a government access request with rigorous scrutiny, ensuring adherence to the rule of law and protection of individual rights.

As we navigate the complex interdependencies of law, technology, and ethics in the topics under discussion in this edition of the GPLR, I also invite the readers to engage with these critical issues. Whether the context is data sharing, AI, smart cities, or financial crime prevention, the principles of fairness, ethical processing, and adherence to the rule of law remain paramount.

Sincerely
Jacques Visser
DIFC Data Protection Commissioner