ISSN 2228-9860 eISSN 1906-9642 CODEN: ITJEA8

International Transaction Journal of Engineering, Management, & Applied Sciences & Technologies

http://TuEngr.com

Privacy Regulations in the Middle East: Challenges & Solutions

Marwan Albahar[1], Mohammed Thanoon[1]

[1]*Department of Science, Umm Al Qura University, PO Box 715, Mecca, SAUDI ARABIA.*
**Corresponding Author (Email: mabahar@uqu.edu.sa).*

Paper ID: 13A5Q

Volume 13 Issue 5

Received 26 December 2021
Received in revised form 15 April 2022
Accepted 23 April 2022
Available online 30 April 2022

Keywords:
Data privacy; Middle East; GDPR; Privacy regulation solution; Cyber security; Right to privacy; Privacy policy; Privacy challenge; Personal Data Protection Law (PDPL); PDPPL; Data privacy issue; Sensitive information.

Abstract

There is a dearth of privacy regulations in the Middle East, which is becoming a real-time issue for businesses in the region. Countries like Bahrain, Qatar, Oman, Saudi Arabia, and the UAE require data privacy regulations as they have faced phishing and malware attacks in recent times. Despite some institutions, such as Dubai International Financial Centre (DIFC) and Abu Dhabi Global Market (ADGM), having their own privacy regulations, the existing data regulations in the Middle East are still in their infancy phase. Considering this in view, the study aims to highlight the challenges of privacy regulations in the Middle East and the solutions provided by these regulations. For this purpose, the study employed a thematic analysis approach and used 16 sources published between 2015 and 2022. It has been identified that the Middle East's data regulations have also offered a secure and safe zone with financial penalties for any organization that violates the law.

Disciplinary: Computer Science and Computer Engineering (Data Privacy & Information Security), Information & Privacy Law.

Cite This Article:

Albahar, M., Thanoon M. (2022). Privacy Regulations in the Middle East: Challenges & Solutions. *International Transaction Journal of Engineering, Management, & Applied Sciences & Technologies, 13*(5), 13A5Q, 1-11. http://TUENGR.COM/V13/13A5Q.pdf DOI: 10.14456/ITJEMAST.2022.101

1 Introduction

Privacy regulation is a term referring to the "right to privacy" of individuals, groups, and organizations [1]. Privacy regulations are important for a state to ensure that all its people and businesses are working in a safe zone with no threat from external sources that could cause data damage, data leakage, or manipulation. According to [2], data privacy is becoming more than a mere security or regulation issue for companies in the Middle Eastern region. Organizations must consider both legal and ethical aspects when using data for professional use. This means that customers, users, and stakeholders may have a lot of SMS marketing messages or numerous emails

that demand personal data sharing. This does not imply that asking for personal data for business use is forbidden under privacy and security regulations. However, it indicates that companies must ensure personal data sharing is conducted through transparency and on fairgrounds of accountability. On the other hand, organizations have shown their concerns about cyber security threats, mainly in the Middle Eastern region [3]. By 2030, the Middle Eastern market is expected to increase as the population grows to 580 million people. The Middle East already owns the largest repository of oil and gas on the globe. It is among the top ten holders of US treasuries and is now viewed for its cultural fame as well as its economic prospects [3]. Middle Eastern countries own the economic prestige of the European region and many other parts of the world. Since the data privacy challenges in Middle Eastern countries are gaining a lot of popularity, companies like LVMH, Hermes, Rolex, and financial institutions have made heavy investments in the Middle Eastern market. [4] claims that the Middle East has been increasingly facing security issues since the start of the pandemic. According to Kaspersky, there are 68 investigative reports in the Middle East, including 29 cyber gangs that are actively targeting Middle Eastern companies. Different countries are working on threat intelligence reports, such as the UAE (49 reports), Saudi Arabia (39 reports), Egypt (30 reports), Kuwait (21 reports), Oman (21 reports), and Jordan (20 reports). On the other hand, Iraq, Qatar, and Bahrain are dealing with less than 20 reports each to address cybersecurity issues. According to [5], there is no federal law in the Gulf Cooperation Council (GCC) that addresses data protection and cybersecurity. ADGM has established its own data protection regulation since 2015. It also launched the Office of Data Protection (ODP) in December 2017 and worked on enforcing regulations. On the other hand, [6] claims that Qatar, Saudi Arabia, and the UAE have recently started focusing on data protection laws and regulations. Qatar has Law No. 13 of 2016 concerning Privacy and Protection of Personal Data (PDPPL) and participated in the first Arab Regional Forum on the Protection of Personal Data. Likewise, Saudi Arabia has published the Personal Data Protection Law (PDPL) in Umm Al-Qura (the official gazette) to develop the first step of its data development [6]. Owing to these challenges, this paper presents the privacy regulations in the Middle East and highlights the challenges and solutions that they offer in the complex contemporary landscape. Therefore, it is important to investigate the challenges and solutions that privacy regulations in the Middle East bring to companies. Such research can be useful for Middle Eastern countries in forming effective policies, enforcing laws, and ensuring that future cyberattacks are responded to with proactive approaches.

This paper highlights the following research questions:

- What are the challenges of privacy regulations in the Middle East?
- What are the solutions provided by the privacy regulations in the Middle East?

There have been few developments and enhancements to the Middle East's existing data protection laws and regulations [7]. This is a growing concern as privacy concerns for businesses grow, resulting in trust issues and debates over how to overcome obstacles. Since data regulation in Middle Eastern countries is still in its infancy, there is little to no research addressing both the

challenges and solutions associated with data privacy in the region. This article combines both data privacy challenges and their solutions for addressing cybersecurity challenges.

2 Methodology

2.1 Context of the Study

Middle Eastern countries are having issues responding to malware, phishing attacks and challenges in social engineering [8]. One such case is the Dubai International Financial Centre, a government body that has enforced its own privacy policy, but since Dubai's law is not as strong as GDPR (EU General Data Protection Regulation), the companies in Dubai that are also working in Europe must face challenges when complying with the EU regulations. Likewise, [9] claims that most of the Gulf countries have been using sharia's principles to protect the data of their users and ensure cyber security. According to [13], the data protection legislation and regulations in the Middle East are in their infancy stage and remain a low priority in the region, where either the data protection laws are very weak or nearly non-existent. However, a lot of Middle Eastern countries, such as KSA and Qatar, are working hard to introduce relevant proposals for the use of technology for data protection. According to [14], almost 71 % of the population in the Middle Eastern region went online in 2019, as compared to 39 % of the population that went digital in 2012. This brings the attention of policymakers, governmental agencies, and administrative authorities to ensure that data protection and privacy regulations are there to protect people from any unlawful or unethical activity that can damage the data recorded. In recent years, data privacy issues and related concerns have increased over time, as illustrated in Figure 1.

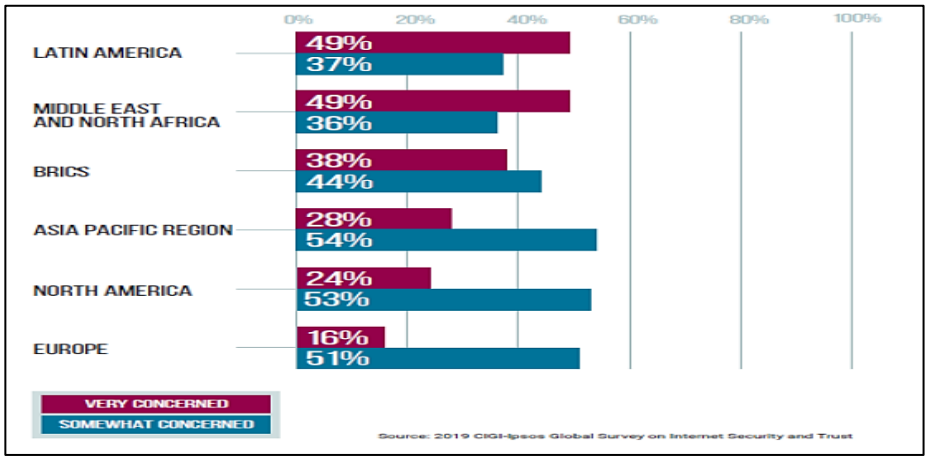

Figure 1: Consumer view on online privacy across the world (courtesy of [14]).

Middle Eastern region has experienced a spike in the number of security incidents (almost 133.3 %) which resulted in 2910 % of files being compromised due to no data protection [15]. At the international level, these surges contribute to 0.7 % breaches of the Middle East. Likewise, [8] reveals that UAE faced three major cyberattacks in 2016, whereas the CERT-ae highlights that the UAE was victimized by malware and phishing attacks in recent years. Thus, the demand for strong and effective data protection regulations automatically emerged in the Middle East to respond to

such security issues. According to [16], both DIFC and the Qatar Financial Centre have developed their own data protection laws and regulations. These data protection laws are quite consistent with EU Data Protection Directive 95/46/EC and even the UK Data Protection Act (1998). However, both Oman and Qatar have more laws related to e-commerce data protection. These include Oman's Electronic Transactions Law (Royal Decree 69/2008) and Qatar's Electronic Commerce and Transactions Law (Law No.16 of 2020). Both laws are based on UN Model Laws pertaining to e-commerce as well as e-signatures. On the other hand, [17] claims that the private companies located in DIFC are following laws enforced by a DPA. Under the DIFC law, the personal information of the individual/group is processed. The information is not shared with any international agencies or a company that does not have compliance with the laws. Exceptional cases such as any protection required from foreign agencies may necessitate sharing of information. In particular, [4] reveals that Middle East's privacy and breach notification regulations are less strict and detailed as compared to those mentioned in GDPR.

2.2 Research Method

The present research employs a qualitative research approach as it undergoes an in-depth analysis of the available privacy regulations that the Middle Eastern region is using and highlights its challenges and solutions. According to [10], the qualitative research approach is useful when study objectives are not based on scientific evidence and statistical data. Since the challenges and solutions are difficult to quantify, a qualitative study approach is used. Moreover, [11] claims that qualitative secondary research may be useful for studies where primary data is either insufficient or difficult to gather. Since gathering primary data from different countries in the Middle East is challenging, the present paper has gathered information through secondary resources. According to [12], a thematic review comprises key themes based on the study objectives.

This research employs two key themes: (i) challenges of the privacy regulations in the Middle East and (ii) solutions provided by the privacy regulations in the Middle East. The main sources of data include databases such as Google Scholar, websites including Jstor, Web of Knowledge, and newspapers such as The Guardian, CNBC, The New York Times, Al-Jazeera, and BBC. 15 sources that have been published in the last 7 years (2015 onwards) are used in this research paper.

3 Literature Review

Various studies have highlighted data regulation challenges that Middle Eastern countries are facing. The study by [7] claims that one of the prominent challenges Middle Eastern countries are facing is the absence of a national data protection law that could provide constitutional rights to the individuals and companies working in the region. Expectations from the Middle Eastern region are high, owing to the region's growing economic importance. In another study [18], it was argued that contact-tracking apps that comprise a large amount of personal data of the user, such as location, health and fitness records, are creating concerns for individuals in the Middle East.

Individuals who were aware that the regions lacked national data privacy regulations expressed dissatisfaction and concerns when using contact-tracking apps during the pandemic.[19] claims that since the Covid-19 applications share data with various stakeholders such as state authorities, health ministries, and other institutions, In the absence of strict data protection laws, individuals are not comfortable sharing their information using apps [20]. This necessitates those digital solutions must be established so that they can address privacy and data security concerns. In another study by [21], it was revealed that the pandemic had increased the cybersecurity and privacy threats for the Qatar 2022 FIFA World Cup. The study by [22] also supports the fact that after the pandemic, cybersecurity threats have increased in the Middle Eastern region, which is giving rise to cyber-preparedness measures prior to hosting events such as the Qatar 2020 FIFA World Cup. [23] have conducted an in-depth analysis to figure out a study to identify and consider cybersecurity threats during Qatar's 2022 FIFA World Cup. The study found that Qatar is taking a proactive approach to addressing emerging cybersecurity issues. Recently, in 2021, Qatar updated these laws, including the Personal Data Privacy Protection Law [24]. The study has also revealed that Qatar is the first Middle Eastern country that has formed a policy related to data protection. Therefore, it is working at the frontline to address cybersecurity issues in the region. In [25], it was revealed that one of the issues that Middle Eastern countries such as Qatar are facing is the interference of security and privacy. Under the smart city regulation, Qatar has already shown its wider interest in overcoming data privacy challenges and regulations. On the other hand, [26] claims that Kuwait has formed a data privacy protection regulation on its official website of the Communication and Information Technology Regulatory Authority ("CITRA") to support the privacy regulation in public and private sectors. Kuwait is struggling to form a unique data protection tool that could effectively regulate the privacy and security concerns in the region.

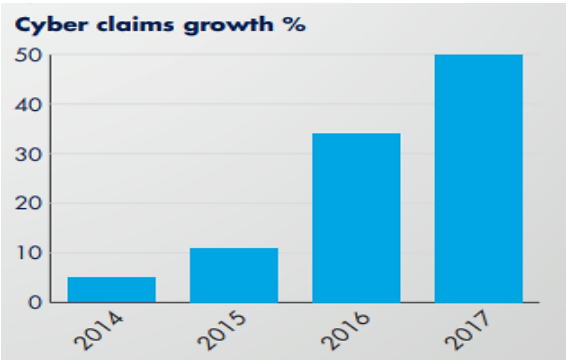

Figure 2: AIG Cyber Claims Report 2018; AIG Europe, Middle East, Africa (Courtesy of [29]).

The work [27] claims that the EU's General Data Protection Regulation (GDPR) came into action on 25 May 2018. Primarily, it replaced the EU's legal framework that was formed in 1995 and provided a regulatory approach with new compliance obligations. GDPR follows an "omnibus approach," implying that it applies to all public and private sector organizations. In contrast to the US legal framework that provides different rules for public and private sector organizations, GDPR

provides a comprehensive data regulation and privacy approach. [28] claims that GDPR offers applicability to companies in the Middle Eastern region without the restriction of having branches or subsidiaries in the European market. The primary reason for introducing GDPR to the Middle Eastern market is to address cyberattacks since there has been significant growth in cybercrimes (Figure 2).

The work [30] claims the regulation applies to all EU citizens and residents, even if they do not reside in the EU. There is a heavy penalty for anyone violating GDPR - up to €20 million or 4% of global revenue. According to [31], the UAE has published its first federal data protection law, which incorporates the majority of the GDPR principles and regulations. The personal data, processing, and controlling techniques have all been extracted from the GDPR regulations for the UAE. According to [32], it is a common perception that GDPR is a more enforceable and effective regulation that, in comparison to the Data Protection Directive, has been robust and applicable since 2018. The Data Protection Directive in the Middle East demands compliance by companies that have a physical presence in the European Union market, such as even a small processing center or server company. However, GDPR does not restrict companies by imposing such limitations and helps businesses show compliance even if they do not have a physical presence in the European Union market. Therefore, GDPR is significant, popular, and applicable in comparison to other privacy laws that the Middle East has formed. Moreover, GDPR protects the personal data of all living beings who have a physical presence in the EU. This includes a person's personal images, contact lists, and even IP addresses [32]. Since GDPR covers such a wide range of personal information for the individual, it is extremely important and effective in protecting the individual's right to freedom and liberty. Therefore, GDRP is popularly known as one of the leading data privacy regulations that are helping companies overcome the challenges of cybersecurity.

4 Results

In light of the literature reviews, the two key themes fulfil the research objectives and depict the following insights.

4.1 Challenges of the Privacy Regulations in the Middle East

The largest obstacle to privacy regulations in the Middle East region is that these laws offer compliance challenges to businesses. Complying with the data regulations could be a challenge for many enterprises and firms that are not yet ready for such a change. Developing a bond of trustworthiness with the clients and customers, as well as getting consent to fulfill the rights of data subjects, proves to be quite difficult for Middle Eastern companies [33]. These data regulations are still in their infancy, which implies that the systems and procedures, along with responses from firms against any actions taken by the relevant authorities (in the case of violating the laws), are still under process. In this regard, [8] has also highlighted that demonstrating the ability of enterprises to manage their data and even provide it to the concerned authorities for protection is a challenging process. It is mainly because the Middle Eastern data regulations mainly have EU GDPR

standards that demand businesses increase their investment in data protection. Likewise, managing to report breach incidents within 72 hours and deciding the leading roles for data protection and privacy are major challenges that companies in the Middle East are facing when complying with data regulations. Furthermore, there is a lack of awareness and skillset required for data regulations and data privacy among companies operating across the Middle East region [16]. In this regard, a similar perspective has been provided by [8], claiming that Middle Eastern companies must ensure compliance with the GDPR by either re-engineering their information systems or developing an adequate privacy assessment and compliance procedure. Thus, this makes the information handling and management procedures quite a complex and sophisticated process that requires a high skill set from the employers.

4.2 Solutions Provided by the Privacy Regulations in the Middle East

According to [34], the Middle Eastern region is expanding business across the world, which results in data privacy issues. Most of the companies in the Middle East also have branches in other parts of the world, such as the USA and the European market. However, with the data regulations introduced by the Dubai International Financial Centre, almost 88 fines have been recorded when companies and groups violated the regulations. These regulations were effective in late 2020, and six new privacy laws were initially enforced in Dubai. These regulations were useful as they included certain extraterritorial laws, including the EU General Data Protection Regulation, and they also had an impact on global and multi-national companies. On the other hand, [33] claims that data regulations have offered countries a critical and crucial opportunity to invest in the Middle Eastern region. The compliance and relevance of certain data regulation laws (KSA and UAE) with the GDPR of the EU is offering a new solution for minimizing issues. These laws provide informational rights, corrective rights, and restrictive rights to businesses. However, the privacy impact assessment, along with assessing privacy risks, is another area that is now given importance due to the new data protection laws in the Middle East. It implies that the data regulations have given businesses and experts in the region the opportunity to consider the aspects when considering GDPR compliance [8].

5 Discussion

The literature review and the key findings of the study reveal that data privacy and regulations are more than just the security and protection of a company's personnel data. Data regulation can even be more complex and may require customers to provide relevant information to the company so that the data can be protected and regulated. From unwanted SMS marketing messages to share customers' personal information with third parties, data privacy may or may not need the consent of the customer. The same is true for clients and business partners, where companies must be completely transparent to ensure that no unethical practices are carried out while data privacy regulations are in effect [35]. Although the key purpose of data privacy is to minimize cyber attacks, malware and phishing attacks, any violation of data privacy regulations may lead to financial penalties for business groups or individuals. This puts the company's

operations, regulators, and customers at risk since any unethical data-sharing activity is reported publicly. The Middle East has seen a rise in business activities and operations that reflect that any company having a wide network of third parties, customers, clients, and business partners may need data security. Typically, the UAE uses DIFC laws, and the Qatar Financial Centre has its own data protection laws [17]. Likewise, ADGM developed its own data protection regulations and even launched the ODP in December 2017. Additionally, Qatar has a Privacy and Protection of Personal Data Law (PDPPL), and Saudi Arabia enforces the PDPL for data protection. This indicates that data privacy regulations and laws are still in their infancy in the Middle East. At such a preliminary level, most of the Middle East laws comply with the EU-GDPR jurisdictions [5, 6]. This creates a complex and sophisticated mechanism where companies in the Middle East must develop skill-sets and roles that can compete with the GDPR rules. The data regulations have given rise to both challenges and solutions for companies and policymakers in the Middle East. One prominent trend highlighted as the challenge is personal data and information sharing with and without the consent of the customer or client. [17] claims that customers' privacy and right to freedom are threatened when companies share their personal information with third parties, especially during marketing activities. As a result, the bond of trustworthiness that is built between the customer and the client is badly affected [33]. Another challenge is investing time, money, and resources for the data regulations to be effectively enforced in the Middle East. Data regulations continue to be ineffective, from finding suitable leadership roles such as CISO, data protection officer, and senior management to developing these leaders' specific skill sets [8]. In other words, the efficiency of data regulations in the Middle East is compromised when the leaders do not have the required skillset, investment, and awareness to enforce and regulate these laws. Despite having compliance that is less strict and complex than EU-GDPR, the data regulations in the Middle East can only be implemented when businesses either re-engineer the information systems or develop an adequate privacy assessment and compliance procedure. [34] also highlights that the ADGM, DIFC, Qatari, and Bahraini laws for data regulation all demand data protection officers to ensure the processing and transferring of sensitive data in the region. It implies that any random employee or organization cannot be appointed to such a leading role. Thus, the leadership should have certain DPO characteristics and skillsets. Therefore, despite having data regulations in the Middle East, companies face challenges when dealing with data privacy issues. On the flip side, the data regulations have also provided an opportunity and solutions to many data privacy concerns. This includes a secure and safe business environment where the companies can conduct their international operations from the Middle East. [33] claims that with the advancement of data regulations in the Middle East, companies are thinking of using AI to act as "privacy concierges" and ensure safe data management and control. Such a system ensures that all unauthorized data transactions are automatically restricted, which saves time and resources in the data protection process. Thus, the data regulations in the Middle East have dragged the attention of policymakers,

business leaders, and experts towards new solutions and opportunities to develop strong and secure data and information handling across the region.

6 Conclusion

In light of the above findings and a review of the literature, it can be stated that the Middle East has been facing data privacy issues mainly because business has expanded in the region. The data regulations in the Middle East are still in their infancy stage, and this has created numerous challenges and opportunities for policymakers, business leaders, and experts. The key challenges that companies face when complying with data regulations in the Middle East are a high investment in terms of money, resources, and time, selecting an appropriate data protection officer with relevant skillset and expertise and ensuring that sensitive information of customers and clients is not unethically shared across various zones. On the other hand, the Middle East's data regulations have also offered a secure and safe zone with financial penalties for any organization that violates the law. Since the Middle East data regulations are less strict than GDPR, companies can accelerate the data handling process by using AI in information handling. Thus, the privacy landscape in the Middle East is quite complex since it complies with the EU-GDPR.

7 Availability of Data and Material

All information is included in this study.

8 References

[1] Data Protection Law: An overview - congress. https://crsreports.congress.gov/product/pdf/R/R45631

[2] PricewaterhouseCoopers, "Navigating data privacy regulations," *PwC*. https://www.pwc.com/m1/en/services/consulting/technology/cyber-security/navigating-data-privacy-regulations.html

[3] The Middle East is a growing marketplace, not just a war zone, Atlantic *Council*, 23-Sep-2020. https://www.atlanticcouncil.org/blogs/menasource/the-middle-east-is-a-growing-marketplace-not-just-a-warzone

[4] Person, "Middle East faced wave of cybersecurity threats since start of pandemic," *Arab News*, 24-Oct-2021. https://www.arabnews.com/node/1953826/middle-east.

[5] A. Coos, "Data Protection Regulations in the Middle East," *Endpoint Protector Blog*, 09-Dec-2020. https://www.endpointprotector.com/blog/data-protection-regulations-middle-east

[6] Middle East data protection update - Taylor Wessing's Global Data Hub, *Home Taylor Wessing's Global Data Hub*. https://globaldatahub.taylorwessing.com/article/middle-east-data-protection-update

[7] N. Pfeiffer, C. Stead, and D. Rosu, "The rise of data protection compliance as a risk - what executives in the Middle East Need to know," *White Label Consultancy*, 08-Nov-2021. https://whitelabelconsultancy.com/2021/06/the-rise-of-data-protection-compliance-as-a-risk-what-executives-in-the-middle-east-need-to-know

[8] G. Nandikotkur and R. Ross, "GDPR compliance in the Middle East: The challenges," *Bank Information Security*. https://www.bankinfosecurity.asia/gdpr-compliance-in-middle-east-challenges-a-9640.

[9] P. S. Report2020-04-28T16:19:00+01:00, "Privacy landscape in the Middle East," *GRC World Forums*, 28-Apr-2020. https://www.grcworldforums.com/privacy-intelligence/privacy-landscape-in-the-middle-east/90.article.

[10] M. J. Coy, "Research methodologies: Increasing understanding of the world," *International Journal of Scientific Research Publications*, vol. 9, no. 1, 2019.

[11] Halim, "Ranjit Kumar Research Methodology a step by step G," *Investigación Bibliotecológica: archivonomía, bibliotecología e información*, 22-Jul-2017. https://www.academia.edu/33999877/Ranjit_Kumar_Research_Methodology_A_Step_by_Step_G.

[12] L. Lawson, S. Clegg, B. Czarniawska, G. Addidle, S. Danby, M. C. A. Lewis, M. H. Allison, D. M. McEachern, M. S. Murray, and M. S. Figgins, "Qualitative research," *SAGE Publications Ltd*, 18-Mar-2022. https://uk.sagepub.com/en-gb/eur/qualitative-research/book245489.

[13] Exposed and exploited: Data protection in the Middle East ..." https://gisf.ngo/wp-content/uploads/2021/02/Access-Now-MENA-data-protection-report.pdf

[14] Regional briefing: Consumer privacy and data protection in Middle East and North Africa https://www.consumersinternational.org/media/314598/privacy-mena-briefing-dec2019.pdf

[15] Breach level index report - privacy *italia*. https://www.privacyitalia.eu/wp-content/uploads/2018/10/breach-level-index-report-h1-2018.pdf

[16] Data Protection and privacy issues in the Middle East, *Al Tamimi & Company*. https://www.tamimi.com/law-update-articles/data-protection-and-privacy-issues-in-the-middle-east

[17] Privacy and security law report - Morrison & forester. https://media2.mofo.com/documents/140428privacylawsinafricaandthemiddleeast.pdf

[18] J. Vitak and M. Zimmer, "More than just privacy: Using contextual integrity to evaluate the long-term risks from covid-19 Surveillance Technologies," *social media society*, vol. 6, no. 3, 2020.

[19] T. Hendl, R. Chung, and V. Wild, "Pandemic surveillance and racialized subpopulations: Mitigating vulnerabilities in covid-19 apps - journal of bioethical inquiry," *SpringerLink*, 2021.

[20] Peer Review #2 of 'Data Privacy during pandemics: A systematic literature review of covid-19 smartphone applications (v0.2). 2022.

[21] H. S. Lallie, L. A. Shepherd, J. R. C. Nurse, A. Erola, G. Epiphaniou, C. Maple, and X. Bellekens, "Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic," *Computers & Security*, 03-Mar-2021.

[22] Towards 2022 – knowledge hub." https://knowledgehub.josoorinstitute.qa/category/towards-2022

[23] N. A. L.-D. Khalifa, "Identification and prevention of expected cybersecurity threats during 2022 FIFA World Cup in Qatar," *Journal of Poverty, Investment & Development*, vol. 5, no. 1, pp.49–84, 2020.

[24] D. Wilkinson and M. Ooijevaar, "Data Protection, Privacy & Big Data 1," *Drone Law & Policy*, pp.183–212, 2021.

[25] A. Badran, "Developing smart cities: Regulatory and policy implications for the state of Qatar," *International Journal of Public Administration*, pp. 1–14, 2021.

[26] S. M. Jr, "Data protection in the Middle East – 2021 regulatory round-up – part 4: Kuwait," *LMI Advisors, LLC - Serving the unique needs of the global satellite industry.*, 29-Jan-2022. https://www.lmiadvisors.com/data-protection-in-the-middle-east-2021-regulatory-round-up-part-4-kuwait

[27] M. C. F. M. C; "The EU's General Data Protection Regulation (GDPR) in a research context," *National Center for Biotechnology Information*. https://pubmed.ncbi.nlm.nih.gov/31314241

[28] PricewaterhouseCoopers, "EU General Data Protection Regulation: Applicability to the Middle East," *PwC*. https://www.pwc.com/m1/en/publications/gdpr-applicability-to-middle-east.html

[29] Aig Care & AIG care. https://www.aig.ae/content/dam/aig/emea/uae/documents/uae-documents/aig-care-brochure.pdf

[30] What is GDPR, the EU's new Data Protection Law? *GDPR.eu*, 13-Feb-2019. https://gdpr.eu/what-is-gdpr

[31] UAE First Federal Data Protection Law, *Global Privacy & Security Compliance Law Blog*, 14-Dec-2021. https://www.globalprivacyblog.com/legislative-regulatory-developments/uae-publishes-first-federal-data-protection-law

[32] How does GDPR affect the education sector in the Middle East?, *Al Tamimi & Company*, 05-Jul-2020. https://www.tamimi.com/law-update-articles/how-does-gdpr-affect-the-education-sector-in-the-middle-east

[33] S. Team, "Impact of modern privacy regulations in Middle East: 10xDS," *Exponential Digital Solutions*, 20-Jan-2022. https://10xds.com/blog/modern-privacy-regulations-in-middle-east

[34] B. Crew, *Amid evolving privacy regulation in the Middle East, stalling on compliance is not an option*, 23-Aug-2021. https://iapp.org/news/a/amid-evolving-privacy-regulation-in-the-middle-east-stalling-on-compliance-is-no-longer-an-option

[35] PricewaterhouseCoopers, "Navigating data privacy regulations," *PwC*. https://www.pwc.com/m1/en/services/consulting/technology/cyber-security/navigating-data-privacy-regulations.html

Dr. Marwan Ali Albahar received his B.S. in computer science from King Faisal University, Saudi Arabia, and his M.Sc. in Computer Science with Honors from Frostburg State University, USA. Dr. Albahar received his Ph.D. from the University of Eastern Finland. Dr. Albahar a senior Information Security, Privacy, and Risk Management Professional with a solid technical background and a highly analytical mind. He has been involved in the information security field for the last 3+. His main areas of research are computer network security, cybersecurity, and artificial intelligence.

Dr. Mohammed Thanoon has taught several subjects in Computer Science and Computer Engineering at Umm Al-Qura University and Tennessee State University. His academic research interests involve the areas of human and machine teaming, data fusion, decision-making, intelligent control systems, artificial intelligence, machine learning, deep learning, federated learning, edge computing, medical image processing, computer vision, robotics, and IoT. He is certified as a "MathWorks Certified MATLAB Associate."