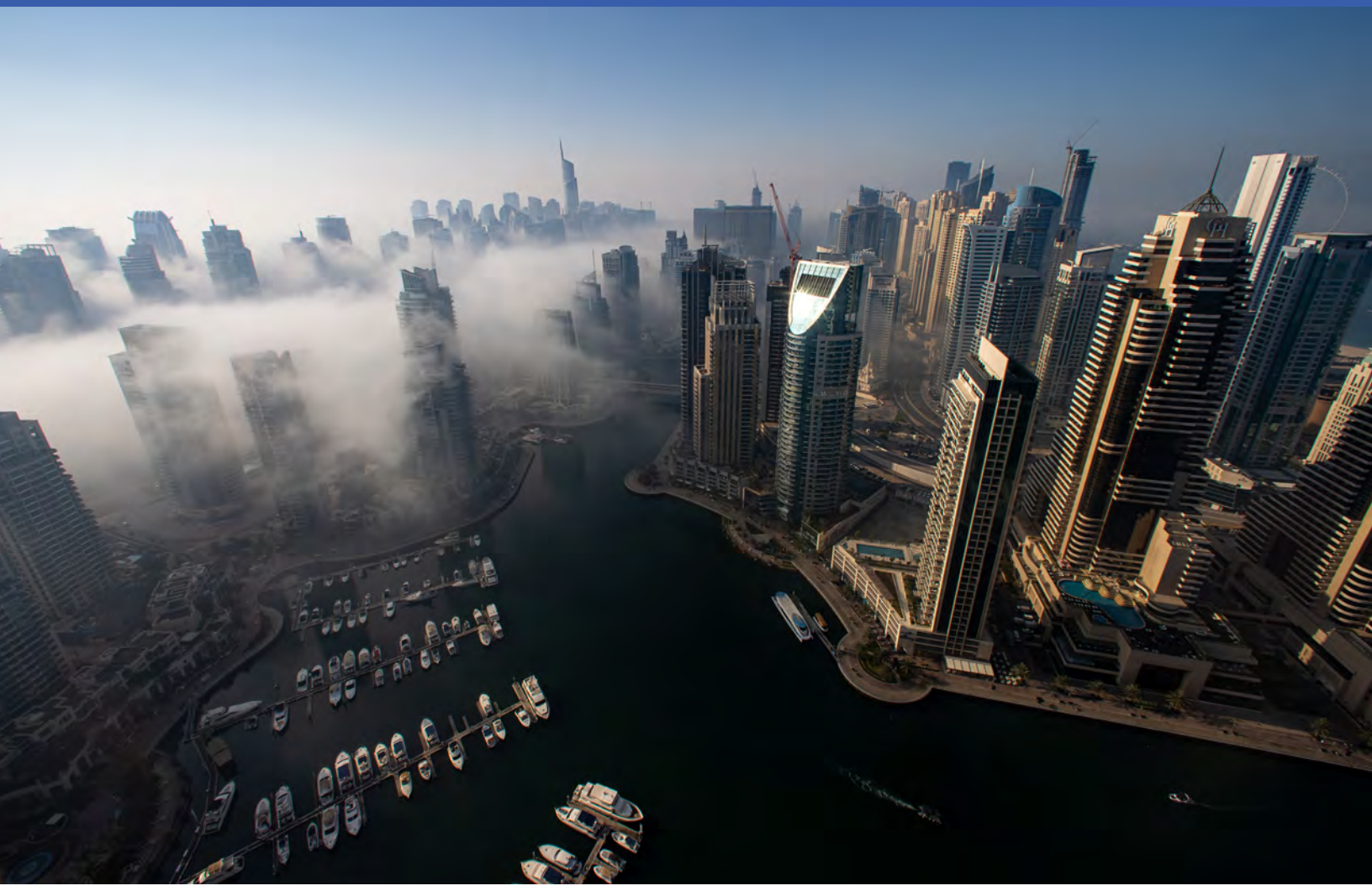
DUST IN THE CLOUD: THE FUTURE OF DATA GOVERNANCE IN THE GCC

THE MIDDLE EAST INSTITUTE

SARAH JOHANSSON & AHMED EL-MASRY

DECEMBER 2021



MEI@75
Peace. Prosperity. Partnership.

WWW.MEI.EDU

ABOUT THE MIDDLE EAST INSTITUTE

The Middle East Institute is a center of knowledge dedicated to narrowing divides between the peoples of the Middle East and the United States. With over 70 years' experience, MEI has established itself as a credible, non-partisan source of insight and policy analysis on all matters concerning the Middle East. MEI is distinguished by its holistic approach to the region and its deep understanding of the Middle East's political, economic and cultural contexts. Through the collaborative work of its three centers — Policy & Research, Arts & Culture, and Education — MEI provides current and future leaders with the resources necessary to build a future of mutual understanding.

ABOUT THE AUTHORS

Sarah Johansson is a Graduate Scholar with the Cyber Program at MEI. Her previous work has considered the international legal remits of state perpetrated and sponsored cyberattacks. She received her LL.B. in Law with a Public International Law focus from Queen Mary, University of London.

Ahmed El-Masry is Graduate Research Fellow with the MEI Cyber Program and a public policy graduate student at the American University in Cairo (AUC). His research focuses on digital policies, cybersecurity, and cyber-politics in the MENA region. El-Masry previously worked as a public policy analyst and as an intern at the European Union Delegation to Egypt and the United Nations Information Centre - Cairo Office.

Cover photo: Morning fog shrouds residential and commercial skyscrapers in the Jumeirah Lake Towers and Dubai Marina districts of Dubai, United Arab Emirates, on Sunday, Jan. 17, 2021. Photo by Christopher Pike/Bloomberg/via Getty Images.

MEI
Policy Center

CONTENTS

ABSTRACT

As the countries of the Gulf Cooperation Council (GCC) work to transform from hydrocarbons-driven to data-driven economies, they will need to make significant and well-planned investments in digital infrastructure, particularly when it comes to the complex issue of data governance. They must take the lead in establishing regulatory and legal frameworks aligned with international standards in terms of data gathering, processing, and storing procedures. This report highlights the existing laws and regulations that govern data protection in the GCC while addressing their potential and limitations, along with the similarities and differences between the GCC's legislative frameworks and the EU's General Data Protection Regulation, and the impact of the GCC's current data protection laws on individuals, the private sector, regulators, and governments.

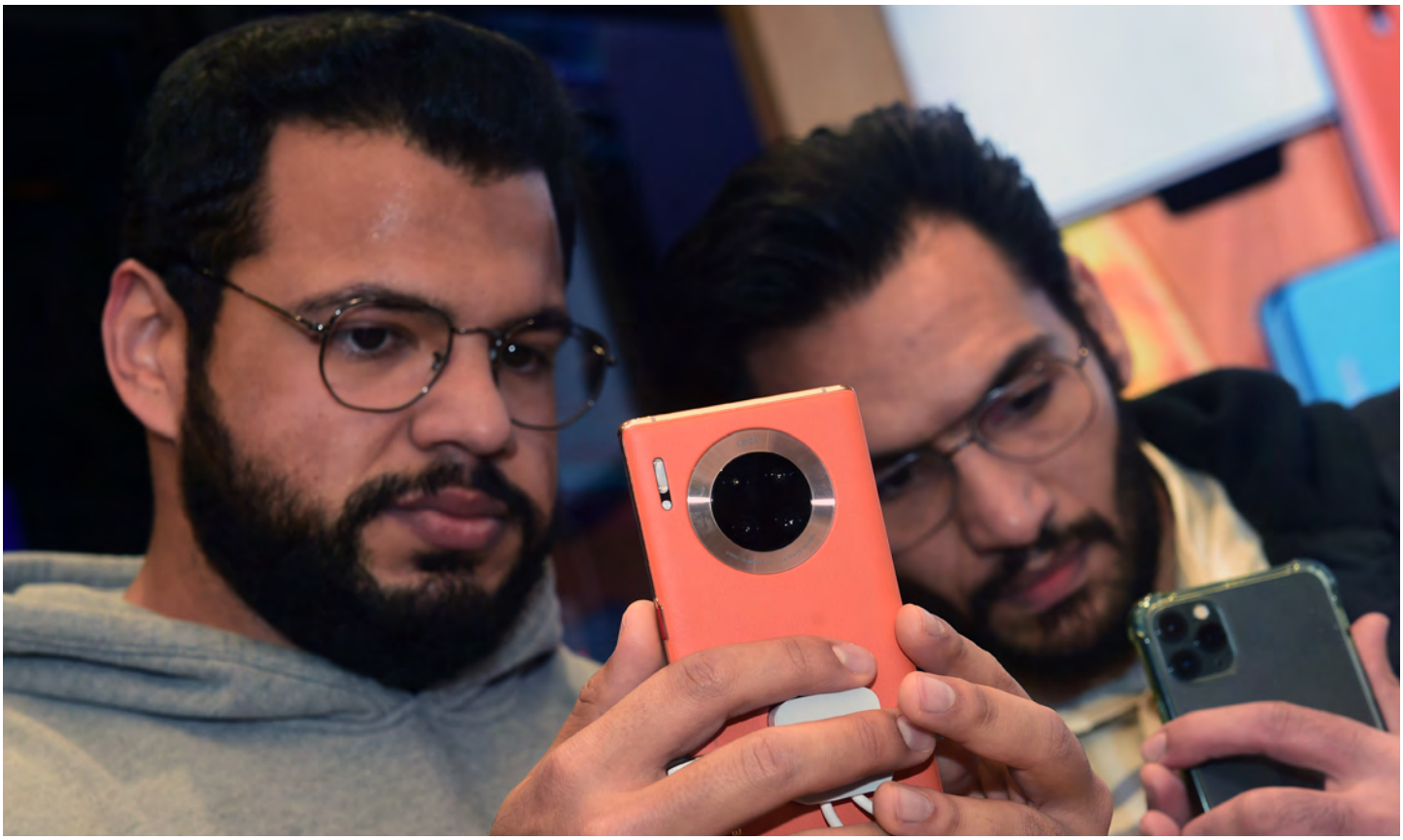


Photo above: Customers try out new 5G smartphones in Kuwait, on Jan. 16, 2020. Photo by Asad/Xinhua via Getty Images.

> **The GCC countries could set an example for the MENA region's further data protection frameworks.**

Introduction

Over the past few decades, the member states of the Gulf Cooperation Council (GCC) have been at the forefront of hydrocarbons production, enabling them to achieve considerable budget surpluses and position themselves as international economic powerhouses. However, these surpluses — and the political and economic gains that come with them — are not infinite, and the looming end of this oil-driven dominance has prompted Gulf countries to rapidly attempt to diversify their economies. The need for diversification is clear and has been borne out by the forecasts of many international financial bodies; in February 2020, for instance, the International Monetary Fund (IMF) argued that the GCC countries could deplete their financial resources as early as 2034 if they continued to follow the same fiscal policies.

“Data governance has a considerable impact on the countries’ economies, business performance, and national security, as well as on critical issues of privacy and information management.”

In short, the need for change is clear. Many GCC countries have built upon their substantial revenues and connections to international business and the technology sector to launch serious digital transformation programs to achieve economic diversification, create more suitable jobs for their young populations, and transform from oil-driven economies to data-driven ones. Accordingly, they have invested heavily in developing their digital infrastructure and capacities. For example, the International Data Corporation (IDC) predicts that the total spending on information and communications technology (ICT) in Saudi Arabia will reach $32.9 billion in 2021. Meanwhile, Emirati ICT spending is expected to increase at a compound annual growth rate (CAGR) of 8%, hitting $23 billion by 2024. Within the broader ICT sector, cloud computing is quickly becoming one of the fastest growing industries in the GCC, with a CAGR of over 25%. By 2025, it is estimated that overall cloud spending by the public and private sectors in the GCC will amount to $2.5 billion.

However, this transformation to data-driven economies requires much more enduring and well-planned investments in digital infrastructure, including paying close attention to the complex question of the governance of data. According to the Data Governance Institute (DGI), data governance is “a system of decision rights and accountabilities for information-related processes, executed according to agreed-upon models which describe who can take what actions with what information, and when, under what circumstances, using what methods.” Data governance has a considerable impact on the countries’ economies, business performance, and national security, as well as on critical issues of privacy and information management. The importance of this emerging field means that GCC countries must take the lead in establishing regulatory and legal frameworks aligned with international standards in terms of data gathering, processing, and storing procedures. By developing comprehensive legislation that obligates the public and private sectors to respect individuals’ privacy, comply with the guidelines, and take accountability for the gathered data, the GCC countries could set an example for the MENA region’s further data protection frameworks. Without a suitable regulatory and legislative environment for data protection and privacy, the GCC will face difficulties in attracting foreign investments and carrying out digital trade activities with several other parts of the world. For example, the European Union (EU) allows the transfer of the personal data of EU citizens only to countries that apply national privacy laws equivalent to the EU standards. As a result, Gulf policymakers and legislators need to update and reframe their existing data protection laws and regulations to be aligned with international principles and standards, as well as specific regional concerns and conditions. Across the GCC, there is a palpable inconsistency in the approaches adopted when it comes to dealing with data protection and data privacy issues. By taking a consolidated and well-managed approach, the GCC will be better prepared to invest in its long-term economic stability, encourage regional development, and fulfill the stated goals of various 2030 economic development plans and other projections for the future.

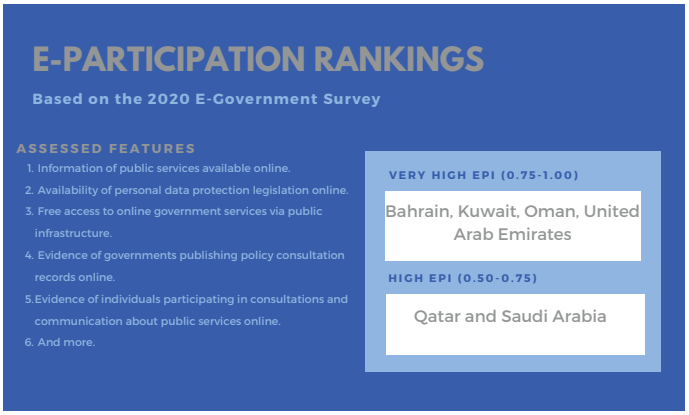
In this report, we will highlight the existing laws and regulations that govern data protection in the GCC while addressing their potential and limitations. We will also illustrate the similarities and differences between the GCC’s legislative frameworks and the EU’s General Data Protection Regulation (GDPR), which is the only comprehensive existing regional legislation to regulate privacy and data protection. Finally, the report will discuss the impact of the GCC’s current data protection laws on individuals, the private sector, regulators, and governments. We aim to identify the key challenges and opportunities for the data industry in the GCC in order to help the region’s policy-makers and legislators establish efficient data governance frameworks that will support their national economic and social reforms.

Existing Data Protection Frameworks in the GCC

The data protection that currently exists in the GCC is set against the reality that many international companies demand

it. When operating within the GCC, these companies insist on data compliance frameworks in line with international rules in order to conduct business with international, and particularly European, customers. Between each country, however, there are varying levels of commitment to data protection in different states and a variety of regulatory environments within the states of the GCC. This stems partly from different attitudes toward international cooperation, distinct and complex views of the concept of privacy as a human right, and the varied pace at which digital services have grown in the region. It is important to note that these differences and the limited application of regional data protection are significant; all GCC countries are among the highest in international rankings of states' digital governance, along with almost all countries in the EU, despite a lack of legislation to protect and regulate this growing market.

Examining how the GCC countries have organized their efforts around ideas of data protection aligned with their particular hopes and needs for the future reveals that each country has adopted a distinct approach, shaped by particular aspirations, concerns, and investments. Although they share many common traits, particularly around the growing role of technology in their economies, GCC countries have chosen to legislate for data protection in different ways. Oman's 2040 Vision, for example, illustrates many of the shared initiatives in the region, while all of the GCC countries (except Bahrain) criminally punish online content that is considered to defy public order and morals with fines and imprisonment. Although there are a number of similarities, the differing strategies between countries when it comes to data protection indicate that the GCC's interests and efforts vary greatly and that a "one-size-fits-all" model like the version approved in the EU's GDPR



The GCC countries appear, according to this metric, to be keeping step with most developed nations for digital government services and access to their citizens. The piecemeal availability of data protection legislation is thus of significant concern.

standards is unlikely to be adopted anytime soon. Additionally, the variance in approaches illustrates the usefulness of understanding a kind of "data protection" timeline, in which states alter their particular investments in data protection in direct correlation with their economic dependence on markets that require it. These differing approaches have been summarized and considered to assess their usefulness today and in the context of an exponentially growing digital economy.

Bahrain

Most prominent in the current Middle East privacy discourse is Bahrain, where there is already a comprehensive Personal Data Protection Law in place. Both the timing (issued in 2018) and content of the legislation is reminiscent of the EU's GDPR. For example, it covers both "standard" personal data and "sensitive personal data" (see Articles [1] and [5]), which accounts for data that would fall under protected characteristics of individuals under EU human rights law. The law also accounts for data movement and regulates the treatment of data if it moves beyond Bahraini borders in Section 3, suggesting an intent to develop laws that allow for international trade and commercial cooperation. This is further highlighted by the development of a fairly unprecedented law designed specifically to ensure that foreign parties are able to safely store data in Bahrain, and the law itself makes reference to cloud-based "data embassies." The focus of these laws is to clarify jurisdictional and procedural rules, such as how a foreign party can request access to data using a court order issued in their own country. Such content has facilitated the engagement of global companies in Bahrain and ensured an avenue for economic growth, not least shown by Amazon Web Services (AWS), one of the world's leading cloud computing providers, opening their first regional data center there in 2019. With some notions of human rights and a framework that many international businesses are already familiar with, Bahrain appears to be taking a safe and business-minded approach. Whether the GDPR-like approach is useful for Bahrain as its economy changes and grows, however, is a question that will only be answered in time.

Qatar

Like Bahrain, Qatar has led the way in implementing data protection laws, introducing the GCC's first such legislation

“In 2019, Bahrain became the first MENA country to host a data center for Amazon Web Services (AWS), one of the world’s leading cloud computing providers.”

in 2016. Law No. 13 of 2016 on protecting personal data is “generally applicable” and focuses on data that is electronically managed and stored. Although reference is made to privacy as a right in the law, the law does not appear to elaborate further on this, nor does it include a section delineating specific guidelines regarding further protection of sensitive personal data. Updates to the law came in 2021, adding further guidelines to simplify compliance for a number of stakeholders. This was aimed at assuring that Qatari companies and other organizations have a clearer picture of what their responsibilities are under the law, as well as enabling foreign stakeholders to better understand what they can expect from those organizations. In commentary about the new changes, Deepak John highlights three significant advantages of this development. Firstly, the updates to the law allow the Ministry of Transport and Communications to hold companies to higher standards and impose significant fines in the event of non-compliance. Secondly, they put Qatar in a “competitive position” for international businesses that are looking for data centers and other services regionally. For example, access to regional data centers will enable a large range of companies to safely store their data locally. This is also true for any business developing a digital service that can now be operated on local cloud servers, providing security and usability. Thirdly, Qatar is, as a result of these developments, becoming a “role model” in the GCC, pushing regional standards of data protection further forward.

Meeza is only one of the large data centers in Qatar, with three locations and a goal to accelerate Qatar’s digital and economic growth in a way that will demand a high level of protection for individual and business data. Qatar seems to be on the right path, demonstrating not only an earlier adoption of data protection legislation than other regional players, but also by paying significant attention to the convenience of those rules for their intended users. Although this could leave the door open to a number of remaining human rights concerns, the approach seems starkly different to much of the criticism of the GDPR’s strenuous application to every aspect of daily life.

Oman

Oman, like most of its GCC neighbors, has recently been investing significantly in data services, such as the government’s cloud hosting platform G-Cloud. In light of this, a substantial data protection law would be of interest to expand the commercial viability of the platform and protect individuals whose data is stored on it, including through those applications hosted via G-Cloud. Unfortunately, Oman has yet to develop such a legal framework and lacks substantive legal protection of privacy as a human right. Although the country’s penal code and basic law cover some aspects of privacy, this is rather limited in comparison with operating a specific protection of privacy as a human right. Instead, a small number of specific laws exist to protect data when collected as part of electronic transactions and under Cyber Crime and general Criminal Procedure law. These provisions protect individuals from malicious actors in relation to theft of data such as payment and postal information. Additionally, the Omani constitution protects communications data from interference. Other data and data accessed by lawful but non-transparent organizations or individuals remain unprotected. Oman thus represents a GCC country with some existing protections of data in place, but a limited availability of human rights and comprehensive legislation that protects and equips individuals and companies alike. This late in the game of data protection as daily global consideration, it seems concerning that there is no clarity as to the path Oman hopes to take in strengthening its privacy laws.

Photo above: Employees work inside the Careem Networks FZ headquarters in Dubai, on Oct. 4, 2018. Photo by Christopher Pike/Bloomberg via Getty Images.

"The Saudi approach focuses on the usability of the legislation by businesses. This sector-specific approach is significantly different from [GDPR] and may signal a trend in the GCC of rejecting general, sweeping regulation in favor of more detailed and targeted legislative provisions."

“The UAE’s flourishing international technology sector signals a business need for data protection but despite this, the country lacks appropriate data protection regulation.”

Saudi Arabia

Despite its more advanced digital economy, Saudi Arabia has only recently begun to take steps toward implementing consolidated data protection regulations. In 2018, the country introduced the Cloud Computing Regulatory Framework, indicating a willingness to develop legislation in new and growing industries. The framework has, however, also been criticized for its broad and sweeping rules on removing any content that may be deemed harmful or unlawful, as well as its rules for businesses to notify the authorities of such content. Particular concern with this stems from the arbitrary nature of punishing individuals who make or distribute content which “‘may’ violate the country’s draconian cybercrime law.” The National Data Governance Interim Regulations of 2020 exist to manage personal data in the absence of more comprehensive regulation, such as human rights, but indicate an initiative to move data protection along in the near future. Although its main focus revolves around government-related data, Part 5 of the 2020 regulation provides some rules that companies and other organizations that act as data controllers (i.e., those which collect and process data) must comply with.

In addition to the limited general application of data protection under the 2020 regulation, a number of sector-specific provisions exist to protect users of cloud services, e-commerce services, medical providers, and more. By equipping global and local companies within these sectors with legislation that can direct their work and instill trust for their customers, the Saudi approach focuses on the usability of the legislation by businesses. This sector-specific approach is significantly different from the GDPR approach and may signal a trend in the GCC of rejecting general, sweeping regulation in favor of more detailed and targeted legislative provisions. As a regional leader in technology and international trade, Saudi Arabia’s sector-specific approach to data protection may also prove a leading and reproducible approach for other regional legislators. While there are promising prospects in relation to Saudi Arabia’s model, more comprehensive data protection legislation is needed in the country and whatever form it takes, it must make room for a fundamental right to privacy.

The United Arab Emirates

The UAE’s flourishing international technology sector signals a business need for data protection but despite this, the country has no general data protection regulation. To some extent, international data is controlled by applicable foreign regulatory systems, but within the UAE, only limited protections exist. There is not a generally applicable definition of data controllers and processors, which exists in some of the more developed legislative data protection frameworks in the GCC. In turn, general legal principles are more difficult to apply where no law currently regulates data usage and storage. There are, however, some requirements of consent as well as rules related to moving certain types of data across borders and regulatory standards of the recipient country. Although the lack of regulation may be beneficial for certain businesses looking to operate in the region, many international companies that have global due diligence requirements may be hindered from working out of the UAE. The Chambers Global Practice guide notes, in relation to the UAE, that “a move to the cloud in the UAE is generally permitted but may require consideration of a number of regulatory regimes depending on the relevant entity’s operations within the jurisdiction.” Further, the existing applicable laws relate to cybercrime and malicious information theft as opposed to protecting data and information more generally (or as a right). The finance, health care, public, and information technology sectors operate some sector-specific compliance frameworks. This provides an opportunity for developing sophisticated frameworks within these and other sectors and could in turn prove a useful model, should it account for privacy as a human right and spread quickly through industries.

Kuwait

Finally, like many of its neighbors, Kuwait's Law No. 20 of 2014 is in place to protect data related to e-commerce. It protects a range of data types from being disclosed by online retailers except where customer consent or a judicial order has been obtained. This may have proved crucial during the COVID-19 pandemic, as an increased segment of the Kuwaiti (and global) population turned to their devices to shop. However, this law only concerns certain types of data while other sector-specific controls exist for businesses in banking and employment. Some concern also exists around the lack of a consent requirement for data collection and storage in Kuwait. The targeted investment into regulation in tech-reliant sectors may be a strategic choice that a number of other regional countries also prefer, namely, to let regulation follow economic growth. This allows investment to boom and then find a steady rhythm as sector-specific regulation creates stability and trust in the markets. Kuwait could, however, also be an indicator of a wider GCC attitude toward data protection should a comprehensive legal framework be adopted. Once the choice between a general, GDPR-like model and a sector-specific approach to data protection is made in Kuwait, it could indicate whether the region is aiming to take the Bahraini or Saudi approach.

GCC vs. GDPR: Comparing Data Protection Frameworks

These examples of data protection regulation in the GCC are most easily compared to the current legal frameworks that have integrated themselves into a region and taken shape globally. The GDPR framework will be at least somewhat familiar to most internet users, and has become a hot topic of discussion among individuals and businesses alike. The daily interaction with data protection policies has mobilized awareness and action for individuals in the EU. But the GDPR has not been entirely fault-free or user-friendly. By comparing the effects of the GDPR and its daily operations to the existing and incoming regulatory frameworks in the GCC, a number of lessons and cautionary tales become apparent. Looking at these different systems and learning from them allows us to present avenues toward better and more forward-thinking data protection regulation.

General Data Protection Regulation 2018

Since 2018, the GDPR has been on most international businesses' radars due to the reach of its data protection principles for any company that has European customers. The reason for its pervasive global reach relates to the foundation of the regulation: a concern for human rights, and particularly the right to privacy. Under the EU's legal framework and after decades of international collaboration, creating a comprehensive framework that protects individuals and their privacy in a time when everything from our entertainment to crucial public services are digital was a win after many long-fought battles in the EU.

In order to introduce sufficient safeguards around digital issues of privacy and personal information, the GDPR framework puts restraints and compliance rules in place for data acquisition, storage, and usage. This involves, for example, requiring a display of a legitimate interest to request certain information and distinguishing between personal and sensitive personal data. Thus, if a website stores information like your home address when you register, but also retains sensitive data on you such as your religious affiliation, that information must be stored and treated differently. Under GDPR, compliance requirements vary and crucially, it differentiates between *controllers* and *processors* of data. Controllers are defined as those who collect data and determine how it should be stored and handled, giving them the primary responsibility and liability for data management. Processors, on the other hand, access and use data for purposes specified by the controllers, without obtaining the data directly from users nor having a say in what the data is used for. The distinction is relevant in the context of the commercial interests of data, but also exists to determine underlying responsibility. Say data is collected and sold by company A, making company A a controller, this will be the first port of call for responsibility in the event of an issue in relation to that data (e.g. a leak, a hack, etc.). The processing company, which may have been assigned by company A to process the data and separate data and personally identifiable information so that certain details can be sold to another company, will be expected to act in accordance with company A's rules and interests. Only where there is concern around company B's lack of compliance would they be held liable on the level of company A. This creates an opportunity for processing

“There are significant disparities between the GCC and the EU when it comes to an integrated approach to data protection.”

companies to exist with a viable profit model, but also creates a chain of responsibility that holds both company A and B accountable to proper protective standards.

A number of industries in the EU have since developed certain sector-specific frameworks to better address the sensitive information that they manage, such as in the health care sector, and to have proper directives for data transfers among different companies to limit profits on gambling addictions without interfering with individuals' privacy. These shifts signaled a need for more thorough and specific standards that not only limit what companies do with data but equip them with tools to build trust and confidence in the business engagement. For long-lasting regulatory and commercial viability, this model seems to set a positive precedent and similar trends have been seen in the GCC.

The GDPR and Data Protection in the GCC

Turning now to the GCC, it is clear that the interactions between different regulatory frameworks stand in sharp contrast to the GDPR. As previously discussed, although a number of larger organizations within the GCC are in many ways GDPR-compliant (for example, by operating websites on which individuals must accept to the use of cookies[1]) and most governments have at least some limited legal frameworks around cybercrime and cybersecurity, there are significant disparities between the GCC and the EU when it comes to an integrated approach to data protection.

At least part of this is simply because of the challenge of creating a widespread and general framework without an already established collaborative relationship between states.

The economic and political environment of the EU is generally organized in such a way as to consolidate economic interests and legislative efforts between states in a shared economic cooperation zone. Meanwhile, despite a number of shared interests among the GCC countries, an equivalent body of governance does not compel such cohesive actions. This lack of a consolidated framework for enforcement, despite shared principles, is one of the main differences between the EU and GCC when considering how to implement data protection. Another critical consideration is the fundamental principle upon which data protection legislation is built. In the EU, privacy as a right is the key to data protection,[2] while in the GCC, protecting individuals from malicious actors and conduct appears to be the first priority.[3] The current differences between the GCC and EU's approaches to data protection do, however, open the door for the GCC to develop more sophisticated data protection, learning from the limitations of GDPR and deploying more reasonably scaled versions of laws that can be iterated and improved upon.

The Lack of a Consolidated Legal Framework

In contrast with the EU, the countries of the GCC lack a shared framework for data protection and national application of rules. Although the union promotes similarities in national regulations on issues such as trade and administration, the data protection regulations in place do not identify a particular regional standard. Most existing frameworks in the GCC are primarily concerned with the threat of cybercrime and creating a robust cybersecurity infrastructure and are mainly designed to put the onus on companies to protect data from attacks, as opposed to establishing a more comprehensive and integrated rights-based system. This is likely to have a significant impact on the willingness of international firms to do business in the

1. Cookies are used to identify you when you use a website and store your data in order to personalize the websites you browse and to make your experience more convenient. Although they are necessary for the kind of digital experience we are used to, they are a concern to one's privacy.

2. See above at page 10, in the discussion of GDPR.

3. See for example the approach by Oman at page 7.

region, leading most European companies toward Bahrain and Qatar, which maintain and operate more robust data protection frameworks, while companies operating in countries with less strict data protection regulations might favor working from the UAE or Kuwait. The real economic impact of this disparity remains to be seen, however; competing approaches to data governance may also provide policymakers with an opportunity to compete with each other to attract international business by developing innovative and future-proof data protection frameworks. Such a development is particularly likely in the GCC, since a number of its economies are heavily investing in their digital economies, with Abu Dhabi's sovereign wealth fund alone pledging at least $2 billion to such industries.

It could be argued that the lack of a consolidated framework is useful and in fact, necessary, to achieve the rapid technological growth that the GCC countries are aiming for. This may ensure that a number of competitors are able to enter the market and facilitate both commercial and socially conscious decision-making by consumers. Where there is room to lead the way in data protective standards, businesses can also find a competitive advantage in committing to high international standards, prompting the wider market to do the same. In this context, it is also possible that efforts can be focused on industries that already require sophisticated data protection regulations, as opposed to prolonging the time before data is appropriately protected to consider a general framework. However, these hypotheses rely heavily on a belief in the forces of the market to achieve a desired result. If it is agreed that data protection is necessary, we must also consider what we will risk to achieve it. In the GCC, where journalists and activists are often silenced and punished as enemies of the state, it is justifiable to ask whether the markets will be free to achieve the necessary standard of protection of privacy as a right. So, let us look at the nature of the existing regulations and whether they may promote a sophisticated sector-specific approach, or if it indicates that a general framework is needed.

Fundamental Principles Behind Data Protection

The majority of states in the GCC lack personal data limitations around identifying, identifiable, and sensitive information on a human rights basis, with Oman as a primary example of the limited implementation of any such principles. The distinction within GDPR that differentiates between "normal" and "sensitive" personal information operates similarly within Bahrain; however, it should be noted that in the EU, under the European Convention of Human Rights, those details and characteristics are much more explicitly protected as part of a larger comprehensive rights framework. This is a relatively predictable distinction between the GCC and EU, given the EU's much more robust and long-standing commitment to human rights. However, this distinction has a crucial impact on individuals in the GCC and beyond.

For example, when data is protected from an attacks-focused standpoint, companies prioritize the defense of data from malicious attackers. When there are concerns with the usage of data from legitimate parties, however, a defense-forward strategy is not likely to be sufficient to protect the privacy and safety of an individual. For example, in countries where homosexuality is, or has become, illegal, the current law enforcement agencies could request or obtain data from organizations or companies that would have that information about individuals within the country. This is particularly problematic for people who may have, for example, registered on a dating app or platform oriented towards LGBTQ users, unregistered a year later, but whose private data is still in the possession of the company. Such information could, under the GDPR, be deleted upon an individual's request and made inaccessible through lawful means. Under an attacks-focused framework, meanwhile, this data could be accessible and used against an individual under scrutiny for years after the fact, with no particular protections in place for that person's privacy or safety. In a commercial setting, the attacks-focused viewpoint is also limiting. A 2019 study on the growth of Big Data in the GCC, for example, showed how further regulatory and governance implementation was necessary to utilize and grow data industries to their full potential in the GCC. The study also indicated that data governance should not only revolve around controlling and preventing misuses of data but should also support additional and improved use of data. In short, an approach that places data purely in a defense and security context, rather than understanding data within a larger framework, will inevitably be less effective, as well as exposing potentially vulnerable people to personal harm.

Photo right: European flags wave in front of the Berlaymont building, the European Commission's headquarters, in Brussels, Belgium, on Jan. 14, 2019. Photo by Michele Spatari/NurPhoto/via Getty Images.

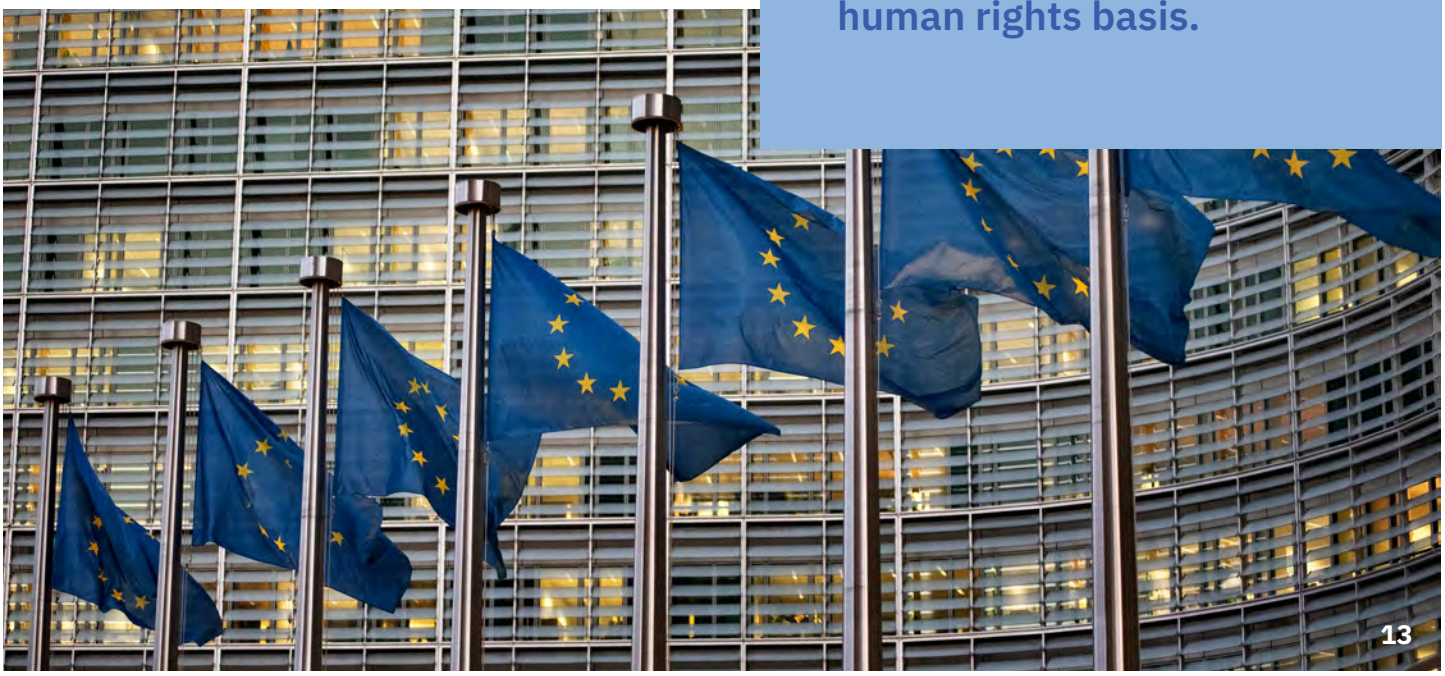
“An approach that places data purely in a defense and security context, rather than understanding data within a larger framework, will inevitably be less effective, as well as exposing potentially vulnerable people to personal harm.”

Leading the Way for Sector Specificity

One of the most distinctive examples of a regionally comprehensive approach to data protection in the GCC is an existing commitment in certain states to the protection of sector-specific data. This is most prominently the case in Bahrain and UAE, which have developed advanced and forward-thinking frameworks for certain key sectors, such as Bahrain’s “Cloud Law” and the UAE’s laws on data protection in the telecommunications and finance sectors. As noted, many of the other GCC countries have also created or adopted some sector-specific rules, including Saudi Arabia. Sector-specificity in this context means developing rules that are applied to a specific sector (such as, for example, telecommunications) to regulate for the needs and concerns of businesses, users, and organizations within that industry. This is a way to set high internal standards with industry usability, help local companies and organizations to become compliant with broader global regulations, and facilitate international operation and cooperation within growing and economically important industries. This will be key to achieving the GCC’s vision of becoming a global technology hub and seems more innovative than the widely applicable fundamentals of the GDPR, which generally is more restrictive in its regulatory framework and application.

Sector specific rules are also significant because they allow private companies to have a direct role in the development of future legislation. This might ensure that new laws are forward-thinking and support individual data protection in innovative ways, but may often have critical implications for how private economic interests, rather than the common good, might most explicitly direct policymaking in this arena. With the significant

“The majority of states in the GCC lack personal data limitations around identifying, identifiable, and sensitive information on a human rights basis.



reach of the GDPR, at least for international companies, creating sophisticated sector specificity may elevate the utility and benefits of data protection worldwide. It should be noted, however, that a foundational layer of general data protection law might be necessary first, for sufficient privacy protection in the GCC. Observers should watch carefully to see how existing data protection regimes in the region may evolve in coming years.

Data by Design: Three Cases of GCC Data Governance in Action

In order to better understand how existing laws and frameworks actually take shape in the EU and GCC countries, it is useful to examine some specific examples of how these regulations have been implemented. In the EU, the GDPR has been tested and the courts appear to have taken the view that very few concerns would override a person's right to privacy. In contrast, examples in the GCC have shown a concern for privacy when infringed upon. These examples highlight the discrepancies between these approaches but also indicate that the GDPR model, although privacy-minded, falls short sometimes. With this, there is room to learn from both models to implement a rules-based framework that sets high standards for data protection — and achieves them.

A Dutch government system designed for System Risk Indication (SyRI) was scrutinized in 2020 for its breach of privacy rights under the GDPR as a result of the data collection and its usage. The system was using large amounts of personal data in order to discern and create profiles of those most likely to fraudulently claim benefits from the government, arguing that the public interest of the system outweighed the privacy risks and concerns. Upon hearing the case, which was lodged by digital rights NGOs, the court found the SyRI system unlawful on balance and as a result, banned it. Privacy International has marked this as a win for privacy rights in the Netherlands and beyond, noting that, "the far-reaching consequences of this ruling are difficult to overstate." The adjudication of these critical, real-life examples of data protection should be watched closely, and may serve as a guiding source of understanding for how governments will prioritize the rights of the most vulnerable in the age of e-governance.

Another example in Qatar reveals how the effects of the COVID-19 pandemic are likely to make issues of data protection in the health sphere of critical resonance for years to come. In mid-2020, it came to light that the country's mandatory tracking application, EHTERAZ, had been released with a security vulnerability that could have allowed attackers to easily access the personal data of over 1 million people, with potential data exposed including names, current location, and health status. Concerns around exposure were quickly flagged, and Qatari authorities remedied the flaw within 24 hours. This served as a warning for many other countries quickly rolling out track-and-trace applications during the pandemic. This case was also an indication of Qatar's attack-focused attitude to data protection, since the security vulnerability was fixed quickly, while additional concerns remain, including about the broader implications of the country's growing trend toward e-governance and the storing of personally sensitive data. The case of Qatar's tracing app shows that an approach to data governance that treats breaches as a public relations or financial threat to be quickly mitigated, rather than part of a longer-term strategy across a variety of sectors, is unlikely to be successful.

The case of the UAE's proprietary national apps for messaging, including the subsequent privacy and surveillance concerns, raises questions about how a nationally mandated approach aimed at protecting governments' autonomy first and foremost is also unlikely to work in the public interest. The UAE government's involvement in the popular ToTok messaging application quickly raised concerns about the inefficiency of local privacy laws after it was released in 2019. It was widely known that the popular app had significant surveillance capabilities and the app's parent company bragged about the application being able to identify faces among billions of videos. Although the application was blocked by both the Google and Apple app stores, the Emirati Telecommunications Regulatory Authority maintained that it was safe to use and that international privacy standards were being upheld. Although Google reinstated the app's availability for a few weeks, it was once again removed in February 2020. The ability for the government to access this data for undisclosed purposes is concerning, particularly in light of the Emirati government's record of repressing human rights activists and journalists, and the reasoning behind developing such an app, likely as a workaround after the country banned VoIP (Voice Over Internet Protocol) apps like FaceTime and WhatsApp. The takeaway from the UAE case? Quick and dirty solutions that

“States have a long way to go in creating robust, well-considered, and effective data protection regimes, both internationally and domestically.”

do not fully take data governance into consideration, including ToTok, are often more trouble than they are worth, and countries should evaluate carefully how to mitigate national security strategies with their competing desires to emulate digital credibility on the international stage.

An example of the GDPR falling short, despite the long-standing commitment to data protection in the EU, was highlighted by the recent ruling in HK vs Prosecution. Despite EU-wide litigation and rule implementation working toward a more thorough and legally clear framework to protect individual rights, significant amounts of retained data in sectors such as the telecom industry remains accessible and retainable to many businesses and governments. Commenting on this preliminary ruling on data retention rules, Ann Väljataga highlighted that although the case did not re-legitimize data retention, it did “relax the general ban on indiscriminate data retention.” This was perceived as a step in the wrong direction by those who are privacy-conscious and considered this a loosening of the adherence to GDPR. Whether this is a sign of GDPR’s limitations or simply a natural legal complexity is debatable. However, it may highlight that an alternative legal solution (to the general notion of data protection) may be preferable to states that are, or are becoming, increasingly privacy-minded.

The varied examples of these cases of data protection in action shows how states have a long way to go in creating robust, well-considered, and effective data protection regimes, both internationally and domestically. With such large aims in the GCC, there is sure to be a significant consideration of the market powers and consumer needs around issues such as privacy. With this in mind, the GCC is a region in which there is a clear opportunity to thoughtfully invest in robust legislation. Whether this opportunity is seized upon, however, remains to be seen.

It is also worth noting that a sector-specific approach has been questioned in the context of the United States. Scholars have argued that reliance on sector-specific legislation, as opposed to a more comprehensive national privacy law, may raise questions about how states prioritize privacy in practice. Emily Wu, for example, argues that consolidated laws bring clarity to consumers and businesses, ensuring that data privacy can and will be a first priority. However, she also promotes the engagement of industry in the development of privacy and security standards, which arguably might be more easily achieved through a sector-specific approach. It may also be the case that the development of international and coherent domestic data governance regimes might be a potential source of goodwill or an opportunity for cooperation between states, particularly if such approaches are framed as an effort aimed at prioritizing the public good. With the changing geopolitical balance of power in the Middle East, including as a result of the Abraham Accords and China’s growing tech diplomacy, this is certainly an area in which goodwill and a more cooperative approach might take root.

GCC Data Protection Regulation: Implications for Individuals, Businesses, and Beyond

Legislation and regulations are designed to supervise and maintain the engagements between different stakeholders while making sure that the rights and interests of each party will be fully respected and protected. Therefore, it is crucial to observe the impact of the existing regulations and laws on the daily activities of individuals, companies, and governments at large, in order to enhance the efficiency and sustainability of the existing frameworks as well as ensure that no one is left behind. When looking at the data protection regulations, it is important to consider the geopolitical elements of the jurisdictions under which these frameworks have been developed. To better understand the various implications of existing data regulations in the region, the following analysis will look into how the GCC’s current data protection frameworks affect the stakeholders involved, in addition to indicating necessary improvements.

Photo above: Visitors chat next to a robot at the GITEX 2020 technology summit at the Dubai World Trade center on Dec. 8, 2020. Photo by KARIM SAHIB/AFP via Getty Images.

Implications for Individual Users

While protecting the right to individual privacy is the fundamental principle behind the driver of the GDPR, in many of the GCC countries, privacy is protected under general provisions of laws that are more concerned with handling pragmatic issues that relate to maintaining cybersecurity and regulating e-commerce rather than focusing on the issues of "data privacy" or "data protection." In an interview, the director of digital trust at PwC, Phil Mennie, argued that there is a limited understanding of how privacy impacts organizations in the GCC region; however, he also maintained that "organisations are finding efficient and economical ways to run their businesses, which involve transferring data outside of their jurisdictions, and are using data analytics to create new revenue streams." Moreover, it was also widely argued that individuals' rights to privacy have been promoted recently in the region due to the interconnectivity of the digital world, which obligates different jurisdictions to comply with the international privacy standards in order to ensure business continuity and encourage international trade activities. Nevertheless, individual privacy should not only be protected because of economic or logistical purposes. In fact, the core motive of enacting data protection legislation should be ensuring that all individuals will enjoy their full basic rights of privacy — not because it is lucrative, but because it matters and is a fundamental human right. Therefore, when dealing with data protection frameworks, GCC policymakers must consider individual perspectives in terms of privacy rights, instead of only focusing on the economic gains or any of the aforementioned pragmatic aspects.

One of the key challenges to the digital privacy of the region's residents is the lack of comprehensive data protection legislation in most of the GCC countries. Apart from Qatar and

“One of the key challenges to the digital privacy of the region’s residents is the lack of comprehensive data protection legislation in most of the GCC countries.”

Bahrain, the GCC countries rely heavily on general provisions of laws that do not specifically address data privacy. For example, in Saudi Arabia, the general legislation that protects individuals digital privacy is the general shari’a principles — the group of general principles and provisions derived from Islamic religious teachings. Accordingly, data protection and data privacy in the kingdom are subject to the general principles of shari’a provisions as well as other sectoral legislative frameworks such as the laws on e-commerce, e-transaction, and cyber-crimes, rather than a specific data protection regulation that comprehensively outlines the issues pertaining to individual privacy. Furthermore, in the UAE, individuals’ privacy is protected under the Penal Code, which makes it unlawful to share news, pictures, or comments that concern other individuals through any platform without receiving their consent. Generally speaking, the major problem with such legislation is that it does not consider the full implications of data privacy and security in the digital age. Legal consulting firms such as Al-Tamimi have indicated that some companies experience legal problems when dealing with situations that require them to transfer employees’ information to data storage facilities located abroad, or when they need to utilize their clients’ data for other commercial purposes that differ from the original use case. In short, it is difficult to ascertain whether such practices are prohibited under the provisions of private information stipulated in the penal codes or not, because of gaps or gray areas in existing legal frameworks. Accordingly, developing comprehensive new frameworks that specifically address all of the issues pertaining to digital privacy and its consequences is a key step on the road to creating and implementing a more robust privacy framework for individuals living in the GCC.

Besides the regulatory and legislative frameworks, a commitment to individual privacy requires more efforts to increase awareness of proper practices to maintain personal privacy in the digital space among people in the Gulf. However, unless users themselves are fully aware of their digital privacy settings and the importance of digital hygiene, it will be difficult for such regulations to be effective at the individual level. Accordingly, reducing the vulnerabilities posed by the lack of awareness about proper privacy practices is essential to maintain data protection in the region. In their study on users’ awareness of privacy issues in Saudi Arabia, AlSagri and Alaboodi indicated that despite the high levels of concern of Saudi online social network users regarding their personal information, these were not reflected in their privacy protection behavior; it was more of a voiced concern than a practiced one. As a result, information campaigns aimed at promoting more of a cultural atmosphere of security awareness for everyday users will be key to any effort to increase protections for individuals in the GCC.

Implications for the Private Sector

Following the issuance of the EU’s GDPR, many of the countries that have strong commercial ties with the EU have shown increasing interest in adjusting their legislative frameworks in accordance with the European legislation in order to create a conducive environment for international business operations. Overall, modern data protection legislation prohibits the transfer of personal data to other jurisdictions unless those other jurisdictions have similar effective legislation in place that protects personal data. Some jurisdictions take the step of clearly listing jurisdictions that could be considered a reliable environment for data protection. As a result, this significantly impacts the companies operating in a specific jurisdiction that fail to comply with the standards applied internationally. For example, in the case of the of the European Commission data protection framework, the “Standard Contractual Clauses” allows for data transfers to take place between data providers in the European Economic Area (EEA) and other data processors that are located outside the EEA, but which are registered in jurisdictions determined by the European Commission based on their compliance with the European data protection frameworks. Interestingly, the European Commission has not yet included any Middle Eastern or African countries on its lists. By looking at the GCC case, it is clear that GCC countries have adopted different approaches to comply

with the new international privacy standards based on the current context and agenda in each country.

As part of their efforts to facilitate the transition to the digital economy, Bahrain and Qatar have introduced the region's first data protection laws, which aim to lead the two countries toward establishing international best practices and guarantee the compliance of businesses operating in their jurisdictions with the GDPR standards. The ultimate goal of this legislation is to attract foreign investments by offering a comprehensive framework for data protection. For example, the main motive behind issuing Bahrain's data protection law was to prepare the country to be the region's hub for data centers, with AWS and Huawei Technologies planning to expand their data centers in Bahrain. For international business operating in Bahrain, one of the key features of its data protection law that will enhance their international operations is the concept of "data embassies," which "enables foreign clients to store their data in Bahrain while ensuring that their data is being subject to domestic laws and regulations in their country of residence as well as those of their country of origin." As a result, this will help the country to foster foreign companies that seek to operate in the region while following the same standards applied in their original jurisdictions. Overall, due to the overlapping nature of contemporary business operations, the existence of comprehensive legislative frameworks in Qatar and Bahrain that clearly outline the rules and conditions for storing, processing, and transferring data will enhance the performance of local and international companies operating within these jurisdictions as they will be compliant with the international protocols and standards that support their cross-border operations.

Meanwhile, the UAE has adopted an approach that does not contain a unified federal data protection legislation; instead, it relies on sector-specific regulations such as the Dubai International Financial Centre (DIFC) Data Protection Law and Abu Dhabi Global Market Data Protection Regulation. In theory, all companies operating in the UAE that offer services to clients based in the EU are required to be compliant with the GDPR as well as the other international privacy laws. However, in practice, establishing a modern federal-level legislative framework in line with international standards is necessary to enable Emirati companies to operate and compete in other jurisdictions around the world. That is why, as part of its attempt to remain a financial hub for the MENA and South Asia regions, the DIFC issued its new Data Protection Law No. 5 of 2020 that replaces the previous Law No.1 of 2007 in order to update its legislative framework to meet the data protection standards applied in other parts of the world, such as the GDPR and California Consumer Privacy Act. This allows international and local companies operating within the DIFC to safely receive and process international data gathered in other countries, which will enhance the efficiency and the competitiveness of Dubai-based enterprises. Nevertheless, issuing similar legislation on the federal level that provides a clear, modern mechanism for data protection will definitely have a positive impact on trade activities across the country, not only for enterprises located in Dubai or Abu Dhabi.

Finally, the lack of specific regulations for the protection of personal data and privacy in Saudi Arabia, Kuwait, and Oman is a serious challenge that undermines the private sector's ability to operate and compete in international markets. Accordingly, in comparison with the other GCC countries that apply data regulations, these countries are less attractive for foreign investors seeking to invest in industries that require cross-border data flows, such as the data center industry and network payment processors. In the context of these countries' plans to diversify their economic activities and transform into data-driven economies, modernizing their legislative and regulatory frameworks to match the international principles and protocols in terms of data privacy and protection will be essential to putting them on the region's economic map as well as helping their private sector compete internationally.

Implications for Governments and Policymakers

Laws and regulations are critical to ensure the protection of personal data and privacy. Nevertheless, they are meaningless unless there are competent regulatory authorities that strive to enforce them. Since data protection laws mostly obligate businesses to be responsible for their data processing activities and guarantee individuals' privacy, the presence of data protection regulatory authorities is vital to supervise the compliance of all relevant stakeholders with the law. Furthermore, regulatory authorities should adopt a principles-based approach, which means that they should observe new trends in technology in order to update and amend the concepts and terminologies of data

“This discrepancy between the GCC countries regarding their approaches to maintaining privacy raises the question of whether this is the time to establish a regional legislative framework for data protection.”

protection laws to align them with emerging technological advancements. This would help to enhance the efficiency of legislative frameworks and their ability to cope with ongoing changes in data-related issues.

Across the Gulf region, the only country that has established an independent regulatory authority for data protection is Bahrain. According to Law No. 30 of 2018, the Bahraini Personal Data Protection Authority is entitled to issue decrees and resolutions pertaining to the implementation of the law’s provisions. However, unlike Europe, the Bahraini authority must report regularly to the minister of justice and Islamic affairs, who could request more information and updates from the authority or empower its staff to execute the necessary functions independently with no need for further approvals from the ministry’s side. Overall, the main responsibility of the authority is to protect personal data by conducting compliance checks on organizations, investigating complaints and violation reports, reviewing requests for the authorization of certain processing activities, and increasing awareness of proper personal data protection practices among different stakeholders. Meanwhile, although Qatar was the first country in the MENA region to introduce a separate data protection law, it has no independent authority that regulates data-related issues. Instead, the Compliance and Data Protection Department of the Ministry of Transport and Communications is mainly responsible for enforcing the provisions of Data Protection Law. Therefore, data contraventions should be investigated by the ministry and in case of any violation the authority is entitled to obligate the data controller or processor to solve the problem and pay a fine.

For the other member states of the GCC, since they do not have specific comprehensive legislation for personal data protection, there are no standalone data protection authorities that focus on tackling issues of privacy and data protection. Generally, privacy is protected through the traditional law enforcement authorities within the scope of the penal code, the civil code, or the other sector-specific regulations that do not mainly address data issues. In Saudi Arabia, because of the absence of a relevant data protection authority, there are no requirements for data protection registration and organizations are not required to hire a data protection officer. Meanwhile, this opens the door for using the technology against human rights, especially against women. For example, Saudi Arabia launched a government-backed mobile app that allows males to track the movement of women as it sends SMS alerts to the paterfamilias when one of the females in the family presents her passport at borders. This obligates females to receive approvals from their male family members before travelling or even getting a job, which strengthens male guardianship in the country.

Moreover, this discrepancy between the GCC countries regarding their approaches to maintaining privacy raises the question of whether this is the time to establish a regional legislative framework for data protection. Despite the common political, economic, geographic, and social factors among the GCC countries, the creation of such a framework does not seem likely. According to Talal Wazani, the head of strategic security consulting at Help AG, the lack of a governing body in the region hinders the implementation of a GCC-wide data privacy law similar to the GDPR governed by the EU and its well-established institutions. As a result, it is quite challenging to align the GCC’s different approaches and transform them into a unified legal framework in the absence of regional authorities that have the power to supervise and regulate data privacy across the member states.

Conclusion

As digital infrastructure grows as the countries of the GCC work to establish economies, societies, workforces, and government services that are increasingly reliant on technology, the broader region is changing. In light of these changes occurring within both governments and private organizations, protection for individuals and their data is

“There is hope that these gaps open avenues for the GCC countries to build strong sector-specific compliance standards that future-proof digital legislation.”

necessary on all levels. While some sectors are so heavily influenced by international business and guidance that they are already compliant with GDPR and other international data protection standards, a fundamental difference in the GCC makes it difficult for other sectors to follow suit. This is the security-based approach to data protection that has pushed many industries to employ security standards around data that protects it from malicious actors. Although this is certainly a step toward data protection, it is not enough.

The rights-based approach employed by the European Commission stands in stark contrast to many of the GCC countries and their approaches to data protection. Although there is concern associated with this lag in legislative protections for individuals, particularly as the data centers industry is booming in the region, there is hope that these gaps open avenues for the GCC countries to build strong sector-specific compliance standards that future-proof digital legislation.

The current limitations include a lack of rights for individuals, limited international reach for regional businesses, and stunted international influence and viability of regional governments in technology discourse. By introducing additional sector-specific legislation to strengthen data protection as concern grows, this paper argues that individuals will benefit and gain the rights they deserve and desire, that businesses will have access to new markets and be able to future-proof their growing capabilities, and that governments will quickly develop a competitive advantage in a globally interconnected marketplace for technology infrastructure, talent, and innovation. A first global standard of data protection has been set — for the GCC countries to truly become digital economies, they will need to match or raise those standards.

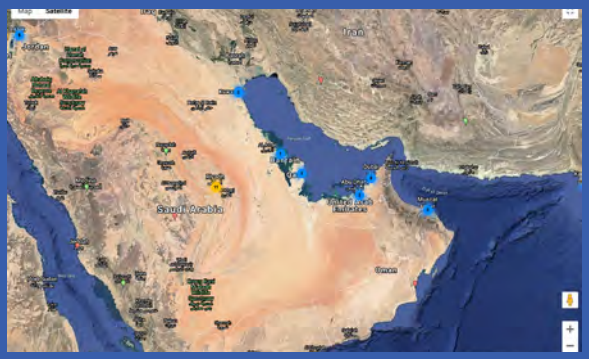
Practical Tips for Stakeholders interested in Personal Data Protection

Individuals

1. **Request information** about the data handling procedures of organisations you sign up with, including encryption, data deletion, etc.

2. **Show concern** for your right to personal data protection in public forums, local government and legislative consultations.

3. Continue to **exercise your rights** with companies that have established data protection frameworks and are GDPR compliant. You can do this by, for example, asking them to remove your data or edit information.



Businesses

1. Employ internal data policies and use these to instil trust with customers and build a secure and valued brand.

2. Request information and infrastructure to achieve data protection frameworks from local governments.

3. Employ accessible tools and guidelines from established Bahraini, Qatari or European frameworks to indicate care for data protection and urging on local development of such frameworks.

Governments

1. Determine and elaborate for transparency on the choice made between a rights-based and security-based approach to personal data protection.

2. Provide local organisations with the information and tools to achieve better data protection, whether with piecemeal and targeted guidance, or general support.

3. Pursue legislative frameworks that will future-proof a growing digital economy and regional data centres.

VISION رؤيـــة 2030

Practical Tips

When considering how different stakeholders might move ahead toward an increasingly privacy-conscious digital economy, there are a few key things that can be done in the lead-up to change.

MEI
Policy Center

MEI@75
Peace. Prosperity. Partnership.

WWW.MEI.EDU