

Kuwait Data Privacy Protection Regulation – Resolution No. 42

The U.S. Chamber of Commerce (“Chamber”) welcomes the opportunity to comment on the Communication Information Technology Regulatory Authority of Kuwait’s (“CITRA”) *Resolution No. 42* on Data Privacy Protection Regulations (“DPPR” or “Regulation”).

The Chamber is the world’s largest business organization, representing the interests of more than three million enterprises of all sizes and sectors, many of whom are major employers and significant investors in Kuwait. In the U.S. and globally, the Chamber is a leading business voice on digital economy policy, including on issues of privacy and data protection, digital trade, cybersecurity, artificial intelligence, and e-commerce. Through the U.S.-Kuwait Business Council, the Chamber engages closely with the U.S. and Kuwaiti governments to advance commercial relations and address policy issues that hinder bilateral trade and investment. In fact, the Chamber hosted Saud Al Zaid, Board Member of CITRA for a discussion in March on recommendations from the private sector on Kuwait’s Cloud Regulatory Framework. CITRA has engaged actively with the Council, including participating in the U.S.-Kuwait Business Council Economic Forum in November. During this event, we hosted H.E. Eng. Salim Muthib Al-Ozainah, Chairmain and CEO of CITRA, as well as H.E. Dr. Sheikh Meshaal al Jaber al Sabah, Director General of the Kuwait Direct Investment Promotion Authority, and H.E. Salem Al Sabah, Ambassador of the State of Kuwait to the United States.

The Chamber commends CITRA for its efforts to advance the data protection of its citizens. The collection, processing, and use of data is a driving force behind the digital transformation of the economy, and a predictable regulatory environment favorable to attracting investors and strengthening industry competitiveness is needed to fulfill the objectives of Kuwait Vision 2035. Given the commercial implications of the Regulation, including on foreign companies’ operations and investment decisions, the Chamber encourages the Government to pursue a privacy regime that balances the objective of protecting consumers’ data with the benefits that data-driven innovation brings, while also aligning with global benchmarks and best practices. The Chamber has developed a set of privacy principles to help achieve such a regime:

Kuwait Data Privacy Protection Regulation – Resolution No. 42

1. A comprehensive framework of regulation that ensures certainty and consistency;
2. Risk-focused and contextual privacy protections;
3. Transparency in the collection, use, and sharing of consumer data;
4. Industry neutrality;
5. Flexibility to develop adaptable, consumer-friendly privacy programs;
6. Harm-focused enforcement;
7. Enforcement that promotes efficient and collaborative compliance;
8. International leadership that promotes the free flow of data and interoperability between global frameworks;
9. Encouragement for privacy innovation;
10. Risk-based approaches to data security and breach notification.

We hope these [principles](#) serve as a set of guidelines for CITRA, as well as other stakeholders in the Kuwait, as it considers further action on data protection. Below, we have identified areas where the Regulation may be improved to facilitate Kuwait's digital transformation, promote bilateral commercial relations, and support data protection. We recommend the following:

Recommendation #1: Embrace a Full Range of Internationally Recognized Data Transfer Tools

The ability to move data and access information across borders is today as important to businesses and consumers as the ability to move goods, services, and capital. Businesses of all sizes and sectors, especially small and medium sized enterprises, rely on cross-border data flows to connect to state-of-the-art global technology platforms and to make day-to-day international commerce possible in the digital age.

The Chamber urges the Government to explicitly recognize a full range of tools for enabling international data transfers within the text of the DPPR itself. These globally accepted mechanisms should serve as independent and legally equivalent bases for transferring personal data out of Kuwait:

Kuwait Data Privacy Protection Regulation – Resolution No. 42

1. **Government whitelists** (“adequacy”) of jurisdictions that possess an essentially equivalent level of data protection;
2. **Model clauses** (“standard contractual clauses” or “SCCs”) are standard sets of contractual terms and conditions which the sender and the receiver of personal data both sign up to, thereby ensuring high standards of protection through contractual obligations in foreign jurisdictions;
3. **Intra-group transfers** (“binding corporate rules”);
4. **Explicit consent**;
5. **Codes of conduct**;
6. **Certifications**; A prominent example of a government-endorsed certification regime is the Asia-Pacific Economic Cooperation’s [*Cross-Border Privacy Rules System*](#);
7. **Public interest**; Such as the transfer of personal health information during the current pandemic;
8. **Necessity for the performance of a contract, and others.**

Global benchmarks such as Singapore’s [*Personal Data Protection Act*](#), Brazil’s [*General Data Protection Law*](#), and the European Union’s [*General Data Protection Regulation*](#) explicitly recognize many of the transfer mechanisms in statute and allow businesses to use whichever tool or mix of tools that meets their specific organization’s needs. Australia’s [*Privacy Act of 1988*](#) also enables organizations to disclose personal information outside of the country and holds them accountable to ensure that reasonable steps are taken to ensure the law’s principles are not breached. These global benchmarks share common roots in frameworks such as the Organization for Economic Cooperation & Development’s [*Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*](#) and the Asia-Pacific Economic Cooperation’s [*Privacy Framework*](#). Importantly, none require the forced localization of personal information, as these measures have not been shown to advance data protection. By incorporating lessons from these international benchmarks, Kuwait will ease the ability of enterprises to engage in cross-border commerce and ensure that regulatory divergences do not serve as impediments to international trade and investment.

Recommendation #2: Remove Onerous Data Classification Requirements

Kuwait Data Privacy Protection Regulation – Resolution No. 42

As written, the DPPR requires private businesses to comply with public sector obligations established in CITRA’s data classification policy. However, these controls and guidelines were designed specifically to manage public sector data, regardless of whether that data is personally identifiable, and do not take into account the operational requirements and processes or sector-specific needs of private enterprises, which differ significantly from those of governments. Extending these requirements to the private sector would be unduly prescriptive without improving data protection or security, resulting in an increase in the cost of doing business, a disruption in business operations, and other material negative effects on Kuwait’s economy that undercut its digital ambitions.

The Chamber recommends that CITRA remove the data classification requirements and instead include a provision requiring that organizations implement “appropriate technical and organizational measures,” such as that found in the European Union’s [*General Data Protection Regulation*](#), to better ensure an appropriate level of information security.

Recommendation #3: Align with Existing Frameworks

While the Regulation lays the foundation for a comprehensive data protection regime, the State of Kuwait has a number of data governance frameworks pending or already in place. These include the Central Bank of Kuwait’s Cybersecurity framework, whose provisions on privacy, security, and classification conflict with those established in the DPPR, affecting sectors such as financial services that are included in the scope of both frameworks. Further, DPPR contains no provision that clarifies whether the new data protection framework would pre-empt any existing guidelines.

The Chamber is encouraged to see the Government striving to adopt a comprehensive framework for data protection. However, it is essential that the Regulation does not exacerbate an already crowded data governance landscape. Rather, the DPPR should align with Kuwait’s existing rules, clearly delineate responsibility between regulators, and not impose different and potentially conflicting requirements on businesses. Indeed, lack of clarity around the scope and application of different frameworks and lack of consistency in guidance and enforcement can lead to challenges for the marketplace, impeding the Government’s goal of attracting foreign investment.

Kuwait Data Privacy Protection Regulation – Resolution No. 42

The Chamber therefore recommends that the Regulation explicitly align with and, where appropriate, pre-empt existing frameworks. Additionally, the Chamber encourages the Government to establish a competent and well-resourced regulator that will operate as a specialized, one-stop shop authority for data protection in Kuwait to avoid uncertainty in the implementation of these requirements.

Recommendation #4: Clarify Definitions

As written, the Regulation lacks clarity in its definitions that could result in confusion for the business community. Currently, there is no distinction between data controllers and data processors, which are collectively referred to as “service providers,” resulting in the imposition of identical responsibilities and obligations on both. We encourage the Government to revisit these definitions and acknowledge distinct functions such as those of data controllers and the processors acting on their behalf. In addition, the DPPR as written uses the terms “user,” “data holder,” “data owner,” and “legal person,” interchangeably without determining who ultimately constitutes the data subject. We recommend that the DPPR provide more precise definitions and use those terms in a consistent manner. We also encourage CITRA look to international benchmarks to help further guide its formulation of definitions.

Recommendation #5: Broaden Lawful Bases for Data Processing

As written, explicit and implicit consent is the primary legal basis to collect and process data under the Regulation. Not only is consent mandatory before collecting and processing personal data, but there are also additional legal obligations imposed as the bases for data processing. We recommend that CITRA consider the benefits of incorporating other legal bases for data processing, which also exist in many international benchmark regimes, such as **contractual and legal obligations**, **public interest**, and **legitimate interest**. Consent is not an absolute guarantee to protect customer interest and is not always feasible for certain types of processing. Relying on consent can also create fatigue for individuals, leading them to automatically accept the terms offered. The fact that consent should always be required for data processing is a “privacy myth.” In many respects, the legitimate interest basis may provide even more protection to consumers.

Kuwait Data Privacy Protection Regulation – Resolution No. 42

Recommendation #6: Refine CITRA’s Scope of Authority

The Regulation envisages broad discretionary rights for CITRA. We recommend that CITRA refine the scope of the authorities laid out in the Regulation so that they are well-defined, transparent, and contain objective criteria. As written, the Regulation grants CITRA the authority to obtain records of data processing without any mechanism for controllers and processors to challenge the request. The DPPR also effectively grants CITRA unlimited physical audit rights to any data controller, processor, and third party, both inside and outside Kuwait, which may undermine efforts to ensure the utmost security of the processing site. The Chamber encourages CITRA to establish due process safeguards to ensure that businesses are able to invest in Kuwait with certainty. We direct CITRA to a Chamber report, [*Seeking Solutions: Attributes of Effective Data Protection Authorities*](#).

Recommendation #7: Embrace a Risk-Based Approach to Data Breach Notifications

The Regulation requires organizations suffering a breach to notify CITRA no later than 72 hours in the event of any data breach impacting personal data. The DPPR also includes a 24-hour notification requirement in the event of improper disclosure of or access to data. These two standards contradict each other and act as an additional source of confusion for industry. By establishing these low thresholds for notification, CITRA will be embracing a regime of *over-notification*, as opposed to one that is based on the risk of real and significant harm to data subjects. If such a standard is not applied, regulators will have a hard time processing and responding to a deluge of breach notifications – even those that do not pose a material risk. Regulators should focus their limited resources on breaches that harm people.

Moreover, the Chamber counsels against the adoption of a 24- or 72-hour notification period, as those require businesses to divert resources away from the important task of investigating and mitigating an active cybersecurity incident to provide regulators with often incomplete or incorrect details. The timeline should instead be made flexible to reflect the real risks that an incident may or may not impact consumers. The Chamber’s [*Seeking Solutions: Aligning Data Breach Notification Rules Across Borders*](#) serves as a resource on risk-based approaches to this issue.

Recommendation #8: Refine Territorial and Material Scope

Kuwait Data Privacy Protection Regulation – Resolution No. 42

As written, the Regulation’s territorial and material scope are overly broad. The Chamber recommends that these be further refined. Extraterritorial application of data protection laws is often difficult to manage for governments and businesses alike and may deter foreign companies from offering goods and services to the Kuwaiti market, due to the ensuing legal ambiguity and risks of conflicting laws. We recommend that the Regulation limit the application of the data protection regime to the data of Kuwaiti persons collected by companies in Kuwait. We also urge CITRA to explicitly exclude data that has been de-identified or depersonalized from the scope of the data protection regime. In doing so, the DPPR will establish strong incentives for enterprises of all sizes and sectors to embrace privacy-enhancing practices, such as anonymization.

Conclusion

The Chamber firmly believes that a well-crafted data protection regulation is the basis upon which sustainable digital growth can be built. We look forward to working with you to implement such a framework, which will facilitate further growth in Kuwait-U.S. trade and investment ties. Please feel free to reach out to us with questions. We would be honored to work with you in the future and will follow up with your office about future opportunities for collaboration.

Contact

Steve Lutes
Vice President
Middle East Affairs
U.S. Chamber of Commerce
slutes@uschamber.com

Sean Heather
Senior Vice President
International Regulatory Affairs &
Antitrust
U.S. Chamber of Commerce
sheather@uschamber.com