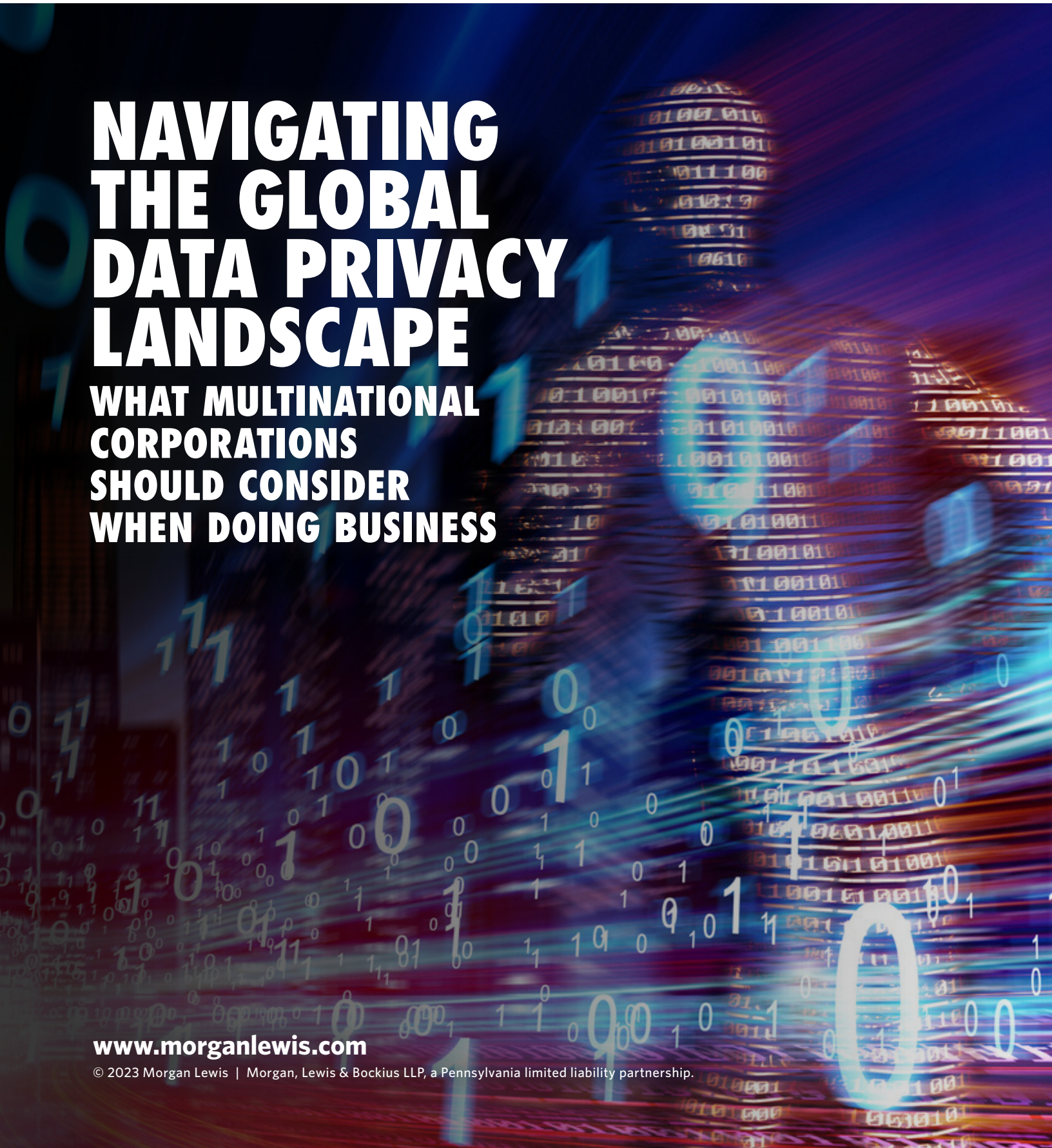
Morgan Lewis

REPORT



NAVIGATING THE GLOBAL DATA PRIVACY LANDSCAPE

WHAT MULTINATIONAL CORPORATIONS SHOULD CONSIDER WHEN DOING BUSINESS

www.morganlewis.com

TABLE OF CONTENTS

Introduction **2**
United States **3**
The European Union and United Kingdom **6**
China **8**
The Middle East **10**
Conclusion **13**
Authors **14**

NAVIGATING THE GLOBAL DATA PRIVACY LANDSCAPE: WHAT MULTINATIONAL CORPORATIONS SHOULD CONSIDER WHEN DOING BUSINESS

The ever-evolving data privacy landscape continues to become more complex as new developments play out on the global stage. In the United States, a number of individual state laws have come into force, with more following in close step, and a new focus is emerging in health data protection. Across the pond, the EU-US Data Privacy Framework became effective and the UK government introduced a new draft of the UK Data Protection and Digital Information Bill. China and the Middle East's approach to privacy continues to focus on cross-border data transfers and adaptations to new technologies, with the Gulf Cooperation Council region attaching significant penalties and enforcement actions in response to violations of the law.

In this roundup of key takeaways from Morgan Lewis's Technology Marathon webinar series, we take a look at the patchwork of privacy and data laws and legislation developing in the United States, the United Kingdom, Europe, China, and the Middle East.

UNITED STATES

States Take Action, With More to Follow

In the absence of comprehensive federal consumer privacy legislation, individual US states have begun charting an evolving course for businesses to follow when handling their customers' data and personal information. While the handful of laws already in existence generally have some commonalities, there are some key variations for businesses operating in different states to be aware of that could make compliance more complex.

- **California Remains the Trendsetter**: The California Consumer Privacy Rights Act (CPRA), which took effect on January 1, 2023, is the most comprehensive consumer-oriented privacy law in the United States. The CPRA adds additional privacy protections to the California Consumer Privacy Act (CCPA), including protections for "sensitive personal information" and the right to opt out of "sharing" data, not just "selling" data. The law also includes privacy obligations for California employers, making it unique among states.
- **Other States Follow California's Lead**: Virginia, Colorado, Utah, Connecticut, Iowa, Washington, Oregon, and Delaware have followed California in setting privacy laws. Each has features that overlap with California but contains its own traits. The Virginia Consumer Data Protection Act (VCDPA) took effect on January 1, 2023, and applies not only to the collection of personal data electronically or over the internet, but also to brick-and-mortar businesses. The Colorado Privacy Act (CPA), which draws heavily from the Virginia law and took effect on July 1, 2023, applies to nonprofit entities. Meanwhile, the Connecticut Data Privacy Act (CDPA), which also took effect on July 1, 2023, does not apply to nonprofits.
    - Utah and Iowa have adopted more business-friendly privacy laws, incorporating terms consistent with the CCPA, but omitting many of the more consumer-oriented terms of the CPRA. For instance, the Utah Consumer Privacy Act (UCPA), which will take effect on December 31, 2023, and the Iowa Consumer Data Protection Act (ICDPA), which will take effect on January 1, 2025, have no requirement for businesses to conduct data-protection assessments.
    - Closest in nature to Colorado's CPA, both the Oregon Consumer Privacy Act, which will take effect on July 1, 2024, and the Delaware Personal Data Privacy Act, which will take effect on January 1, 2025, have broadened definitions of "sensitive data" as well as a broader definition of "sale" that includes the exchange of personal data for monetary consideration and "other valuable consideration."
- **State Laws Broadened to Address Health Data**: Connecticut has added new requirements to the CDPA and Washington State has passed standalone legislation called the My Health My Data Act to give consumers more control over how businesses treat information about their health and the data of youths. The amendments to the CDPA will provide individuals with rights over their personal information that include accessing and correcting what companies collect. These are already in effect, while the provisions pertaining to youths will come in 2024. Described as a "gap-filler," the legislation will have an impact on the privacy practices of a wide range of digital health businesses and potentially reach beyond the state's border. While the act takes effect on March 31, 2024 for regulated entities and June 30, 2024 for small businesses, the act's geofencing provision became effective on July 23, 2023.

Similarities and Key Fault Lines

One deficiency that all states share is a lack of private right of action, save for California's limited private right of action related to security breaches. Thus far, states have allowed their respective attorneys general or other regulators, rather than consumers, to file complaints and enforce the laws. The states

each allow consumers to access their data and delete at least some data, require privacy notices, and have special requirements for children's data.

However, there are a few key differences for businesses to be aware of, including the following:

- California has a broad expansion of the law to cover employees. Most states focus on "true consumers," not employees or business contacts. That is a key distinction and complicates compliance in California.
- Virginia, Colorado, and Connecticut are more restrictive than California with respect to requiring sensitive data consent in advance and prohibit processing of sensitive data without first obtaining the consumer's consent. The CPRA, UCPA, and ICDPA contain no comparable opt-in requirement, but California, Utah, and Iowa have the right to limit the use of their sensitive personal data by submitting a request to a business.
- Virginia, Colorado, Utah, and Connecticut give consumers the right to opt out of, and require controllers to disclose, the processing of personal data for the purposes of targeted advertising, while Iowa lacks such a requirement. Meanwhile, the California law addresses "cross-context behavioral advertising" and treats sharing of personal information for that advertising in the same way as a "sale" of personal information under the CCPA.

Learn More

In our recent Technology Marathon presentation New State Consumer Privacy Laws, we discuss the latest developments in state consumer privacy legislation and consider how businesses can meet the challenges of a US privacy regulatory landscape that is growing increasingly complex. Leverage our US Privacy and Data Protection Law Tracker to stay up to date on the latest data privacy laws in the United States.

Could a Federal Law Be on the Horizon?

Despite the business community's interest in an all-encompassing federal data privacy law, such a development remains elusive. US legislators have periodically introduced bills that would establish a federal data privacy law, but none have been put into action. The American Data Privacy Protection Act, introduced in May 2022, was the latest attempt to establish a federal privacy law while providing for limited preemption of state privacy laws. The measure has enough bipartisan support to make it out of committee, but chances for passage are unclear, as it appears to lack key support to move further. Nonetheless, 2023 looks to be continuing the trend of increased attention on data privacy and security by the US Congress and federal agencies.

Federal Communications Commission

We expect the Federal Communications Commission (FCC) to continue its focus on enforcement this year, particularly with respect to recipients of federal funds such as the Universal Service Fund and other loan and grant programs that the agency administers. Policy initiatives will continue to focus narrowly on national security, consumer protection issues such as preventing robocalling, data security, and privacy investigations, at least while the FCC remains deadlocked with two Republican and two Democratic commissioners.

Calls to reform Section 230 of the Communications Decency Act have increased, with criticism from both sides of the political aisle. With uncertainty on the scope of the FCC's authority to interpret Section 230, the agency likely will continue to defer to Congress. The US Supreme Court recently resolved a pair of cases testing Section 230 liability protections for online platform providers, with the online platforms prevailing.

Federal Trade Commission

The Federal Trade Commission (FTC) first addressed artificial intelligence (AI) in 2016, but the agency's pace in addressing AI-related issues increased markedly over the last year. On August 11, 2022, the FTC released an advance notice of proposed rulemaking (ANPRM) seeking preliminary comments relating to commercial surveillance and data security—one of the agency's most comprehensive and ambitious rulings.

The ANPRM's sweeping scope sought public comment on a wide range of issues, including protection of minors, data privacy, data security, algorithmic discrimination, and AI-related concerns. The ANPRM is one step in a lengthy process, and the deadline for public comment closed on November 21, 2022.

Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act (CFAA) is one of the few statutes addressing privacy and data protection at the federal level, where it imposes criminal and civil liability on anyone who "intentionally accesses a computer without authorization or exceeds authorized access." Website owners have used the CFAA as a method for prohibiting unauthorized data collection from their websites, a practice referred to as "data scraping."

A recent court decision narrowed the CFAA's scope, finding that, under certain circumstances, the act is inapplicable to situations where users with legitimate access misuse such access. Separately, another recent decision rejected CFAA-based claims where a website operator made certain information public but attempted to restrict a particular company's access to said information. In these instances, other causes of action may still apply, such as common law claims of trespass, copyright infringement, breach of contract, unjust enrichment, or conversion, or claims under state-specific statutes.

Congressional Activity Related to Privacy

The following privacy-related legislation has been recently introduced in Congress.

- American Data Privacy and Protection Act: Passed the House of Representatives' Energy and Commerce Committee in a 53-2 vote, with the intention of providing consumers with foundational data privacy rights, creating strong oversight mechanisms, and establishing meaningful enforcement. The bill will require a reintroduction and restart to its legislative path in the House. On March 1, 2023, the House Subcommittee on Innovation, Data, and Commerce held a hearing to restart the process. The bill largely preempts state laws, but not all of them.
- Data Privacy Act of 2023: Aims to modernize the Gramm-Leach-Bliley Act to better align with the evolving technological landscape. The bill addresses the privacy and security of personal information held by financial institutions and expands the application of current protections, provides individuals with controls for limiting the collection of their information, and establishes data privacy standards nationwide.
- Upholding Protections for Health and Online Location Data (UPHOLD) Privacy Act: Designed to prevent the use of personally identifiable health data for commercial advertising. It would place additional disclosure restrictions on companies using personal health information without user consent and ban the sale of precise location data.

Learn More

In our recent Technology Marathon presentation Hot Privacy and Data Security Issues on the Hill and at the FCC and FTC, we cover the latest privacy and data security developments on Capitol Hill and with federal agencies.

THE EUROPEAN UNION AND UNITED KINGDOM

International Data Transfers

The governance of international transfers of personal data continues to develop in the European Union and the United Kingdom.

Given the relative strength of the General Data Protection Regulation (GDPR) in comparison to privacy legislation in other countries and regions, EU- and UK-based individuals risk losing the protection of their personal data under European privacy legislation when their personal data is transferred to other countries. As a result, the EU and UK GDPR contains rules for international transfers of personal data where the receiver is a separate controller or processor and legally distinct from the exporter. If the transfer is not covered by an adequacy decision, the transfer must be covered by an appropriate safeguard. One commonly adopted example of an appropriate safeguard is the European Commission–approved EU Standard Contractual Clauses (SCCs).

- **New EU SCCs**: Following the Court of Justice of the European Union's judgment in the high-profile *Schrems II* judgment, the European Commission issued modernized SCCs under the EU GDPR, replacing the three sets of SCCs that were adopted under the previous EU Data Protection Directive. These went into effect for controllers and processes on December 27, 2022.
- **UK Standard Contractual Clauses (UK SCCs)**: In light of Brexit, the new EU SCCs were never valid for use with respect to UK personal data transfers outside of the United Kingdom to third countries. Controllers and processors were expected to rely on the prior version of the EU SCCs until the UK published its own version. On February 2, 2022, two sets of UK SCCs were laid before parliament: (1) the new International Data Transfer Agreement and (2) the new International Data Transfer Addendum to the EU SCCs.

EU-US Data Privacy Framework

The EU-US Data Privacy Framework (EU-US DPF) became effective on July 10, 2023 and, on the same day, the European Commission adopted an Adequacy Decision relating to the DPF. As a successor of the EU-US Privacy Shield, the EU-US DPF facilitates the transfer of EU personal data to participating organizations in the United States. Only those companies subject to the jurisdiction of either the FTC or the US Department of Transportation are eligible to self-certify their compliance with the EU-US DPF. The scope of eligibility is likely to broaden in the future.

One week later, on July 17, the International Trade Association, within the US Department of Commerce, launched the DPF program website. While organizations may voluntarily certify their compliance with the EU-US DPF or the Swiss-US DPF (once it becomes available—likely this fall) if they choose, in order to participate in the UK extension to the EU-US DPF, organizations must participate in the EU-US DPF. The EU-US DPF triggers a range of compliance obligations for various organizations, including making updates to privacy policies and registration processes and ensuring dispute resolution under the EU-US DPF by data recipients. US organizations subject to the GDPR must comply with it irrespective of their participation in the DPF program as it instead provides a mechanism for the transfer of EU personal data from the EU to the United States.

Other Developments

Risk Assessments: Controllers and processors that transfer personal data outside the United Kingdom or European Economic Area (EEA) under an Article 46 UK/EU GDPR transfer mechanism must carry out a transfer risk assessment (TRA). The UK privacy regulator published new guidance on TRAs on November

17, 2022. The intention behind a TRA is to evidence that the transfer mechanism selected will provide an appropriate safeguard as well as effective and enforceable rights for data subjects.

Data Breach Developments: The Information Commissioner's Office (ICO) recently announced a change in its approach to publishing reprimands. In the past, companies could typically rely on their dealings with the ICO regarding data breaches being kept confidential. This is no longer necessarily the case. In early December 2022, the ICO published its reprimands from January 2022. Some of the information now publicly available includes details of organizations' data breaches and resulting reprimands.

Analytical Cookies: Interest in the use of analytical cookies has increased over the last year following complaints from None of Your Business (NOYB), an Austrian nonprofit organization established with the aim of strengthening individuals' privacy rights. NOYB has issued complaints in all 30 EEA member states against 101 European companies. Many tracking technologies commonly used on websites in the EU are offered by companies based in the United States.

NOYB has claimed that personal data has been transferred to the United States using Google Analytics and Facebook Connect in violation of the GDPR. This has resulted in several regulatory decisions being issued in the European Union, and largely faced scrutiny from several European regulators, including those in Austria, France, Italy, Germany, Liechtenstein, Norway, Denmark, and the Netherlands. This pattern is expected to continue into 2023. Corporations should be analyzing their cookies use—particularly any use of Google Analytics—to mitigate enforcement risks and adapt accordingly while monitoring developments.

EU AI Act: The European Parliament voted on June 14, 2023 to adopt its position on the draft EU Artificial Intelligence Act (the EU AI Act), which would impose a comprehensive regulatory regime on AI. More rules are expected to follow for companies based in the United States. Currently, certain laws in the EU and EEA apply to AI, particularly the GDPR, which includes provisions applicable to products and services using AI technologies such that companies must consider the GDPR when using AI systems to collect or process personal data of individuals located in the EU and EEA.

- In addition to the applicability of the GDPR to AI products and services, the European Commission continues to address AI holistically. Provisions in the draft EU AI Act include stricter requirements for generative AI services and an expansion of the scope of what are considered "high-risk" scenarios.
- If the EU AI Act survives in its current form or close to it, the EU would adopt the strictest approach with respect to regulating AI systems compared to the United States and the United Kingdom.

UK Data Protection and Digital Information Bill: On March 8, 2023, the UK government introduced the Data Protection & Digital Information (No. 2) Bill, withdrawing the Data Protection & Digital Information Bill that was introduced in June 2022, yet paused. The bill is intended to make the GDPR more practicable and less onerous in lower-risk situations, while simultaneously maintaining high standards of data protection. The new bill contains various clarifications from the 2022 bill, and may take up to 12 months before it becomes an act.

Learn More

We discuss the latest laws, regulations, and guidance covering privacy principles throughout Europe and the United Kingdom in our Technology Marathon presentation and Global Privacy Year in Review report.

CHINA

China has garnered significant attention in terms of its privacy and security legislation in recent years. For multinational corporations operating in China, the three most pivotal legal frameworks governing data protection are the Cybersecurity Law (CSL), which took effect in 2017, the Data Security Law (DSL), and the Personal Information Protection Law (PIPL), both of which took effect in 2021. These laws lay out China's legal framework for enhancing data protection supervision, specifically with respect to data that will impact national security and data security.

Government authorities, such as the Cyberspace Administration of China (CAC), have promulgated a myriad of regulations to effectuate the above-referenced laws. In addition, other government and semi-government agencies, such as China's National Information Security Standardization Technical Committee, have also issued national standards to provide further elucidation. Furthermore, additional implementing regulations and national standards are currently in the process of being drafted or are yet to be finalized.

In addition to the PIPL, CSL, and DSL, the following legal instruments form the foundation of the existing personal information protection framework in the People's Republic of China:

- Measures for the Standard Contract for Outbound Transfer of Personal Information, effective as of June 1, 2023
- Measurements for Security Assessment for Cross-Border Data Transfers, effective as of September 1, 2022
- Implementing Rules for the Certification of Personal Information Protection, effective as of November 4, 2022
- Draft Regulation of Network Data Security Management, released for comments on November 14, 2021

Over the last five years, there has also been a number of national standards and other guidelines issued that, while highly persuasive, are serving as technical guides and thus are not legally binding. While the PIPL takes priority over the specifications and guidelines, the latter still perform an essential role in supplementing the existing legal framework, especially with respect to any aspect that has not been fully elucidated by the PIPL, CSL, or DSL.

Cross-Border Data Transfers

As noted above, the long-awaited final version of the Measures for Security Assessment of Cross-Border Data Transfer states that a data handler (a concept similar to a data controller under the GDPR) must declare a security assessment for its outbound data transfer to the CAC if any of a number of thresholds are met.

If the data handler does not meet any of the thresholds above for the security assessment, the data handler should follow one of two procedures before lawfully transferring personal information outside of China: (1) enter into a data transfer agreement with the overseas data recipients based on the standard contract published by the CAC or (2) obtain a personal information cross-border transfer certification from a "qualified institution" (designated as the first certification agency under the PIPL, the China Cybersecurity Review Technology and Certificate Center will be valid for three years and can be renewed if relevant requirements are satisfied).

Recent Updates on Important Data Identification

The DSL provides special protection of important data; however, it does not specify the scope of important data, and instead leaves the detailed catalogs to be developed by relevant regions, departments, industries, and fields.

From July to December 2022, the CAC, together with the general office of the Shanghai government, set up a pilot working group to organize the pilot work of classifying and grading data and developing important data catalogs.

On May 18, 2023, the CAC released Important Data Identification Rules (the Rules), which are the pilot result of the Shanghai New Energy Vehicle Public Data Collection and Monitoring Research Center for data classification and important data catalogs development in the field of new energy vehicles.

- The Rules describe the process for identifying important data and serve as a catalog of important data for the new energy vehicle industry in Shanghai.
- The Rules are not binding on other industries and are not binding on companies outside of Shanghai. The Rules are the Data Center's practice under the DSL and are published by the CAC as a model for identifying important data, which has great significance for the reference of the identification and management of important data in other regions and other industries.

Learn More

In our recent Technology Marathon presentation China's Privacy and Cybersecurity Regime: What Tech Companies Need to Know, we provide an overview of China's PIPL, DSL, cross-border data transfer measures and their impact on the technology industry, cross-border transfer of data and technology, and relevant data privacy compliance issues.

THE MIDDLE EAST

The Gulf Cooperation Council (GCC) region's heavy focus on technology and innovation is dictating how privacy laws are administered, placing emphasis on protecting and supporting the rights of consumers, employees, and other data subjects.

Regional Trends: A Practical Approach

Despite the GCC's data privacy legislation being enacted relatively recently, one major benefit was that the collective governments were able to observe guidance, frameworks, and legislation from around the world and collect and implement the best practices and most recent developments into their own laws. Collectively looking at the GCC region's approach to data protection laws, some common emerging themes include:

- **Data protection laws and enforcement practices are rapidly developing** and are often based on best international practices, such as the EU's GDPR.
- **Enforcement is taken very seriously**. Liability exists in every jurisdiction and is very severe, with penalties for violations ranging from fines to criminal charges to imprisonment. That said, the enforcement practice is still uneven.
- **New technologies are being captured into law**. New technologies, such as AI and facial recognition, are either captured in new laws being issued or captured in existing laws that are being amended to address these new advancements.
- **Control over cross-border data transfers and extraterritorial reach are highly regulated**. In practically every country of the GCC region, cross-border data transfers require additional consideration and, in certain cases, approval from the local authorities.

The United Arab Emirates

Some commonalities among the general framework for the emirates include the common allowance of cross-border data transfers to adequate and nonadequate countries, the appointment of a data protection officer (DPO) in certain cases, and taking a risk-based approach when implementing appropriate technical and organizational measures for data protection.

Federal Decree Law No. 45 of 2021 on the Personal Data Protection

- While it formally came in force in January 2022, the Executive Regulations have yet to be released. Once issued, there will be a six-month grace period for compliance. The law has extraterritorial reach, except in instances of government data and government authorities (companies) that process data and data held with security and judicial authorities.
- Processing of health data, banking, and credit data is exempted from the privacy law and is regulated by other UAE laws.
- Other notable features include the mandatory maintenance of recording processing activities and the immediate reporting on data breaches to the UAE Data Office.

Privacy Legislation of Free Economic Zones

- **Dubai International Financial Centre (DIFC)**: Applies to companies registered in the DIFC and those registered elsewhere if they process data in the DIFC as part of the so-called "stable arrangements." It could potentially be amended soon to address data use in AI, digital, and communications services and apps. Violators could face warnings, public reprimands, and fines of up to $100,000.

- **Abu Dhabi Global Market (ADGM)**: Applies to data processing in the context of activities of an establishment of a controller or a processor in ADGM, regardless of where the processing takes place. Data controllers must register with the Office of Data Protection at the Registration Authority and pay a data protection fee, plus renew on an annual basis. Violators could face significant fines for noncompliance of up to $28 million.

The Kingdom of Saudi Arabia

The Personal Data Protection Law was recently amended and will be effective as of September 14, 2023. It includes a one-year grace period for compliance. The law has extraterritorial reach where the law applies to all personal data processing in the Kingdom of Saudi Arabia (KSA) and all personal data processing undertaken outside the KSA in respect of data subjects in the KSA. Violators will face significant fines of up to $1.3 million for noncompliance.

Notably, the strict prohibition on transfers of personal data outside Saudi Arabia has been amended, and international transfers may no longer require exceptional approval from the Saudi Authority for Data and Artificial Intelligence (SDAIA). While no registration is required, the SDAIA will issue the requirements for practicing activities related to data protection and will license auditors and accreditation entities, as well as maintain a national register.

The Sultanate of Oman

The Personal Data Protection Law has been in force since February 13, 2023. The law does not include the concept of legitimate interest, and express consent is usually required for data processing. Notably, there is an obligation to appoint both a DPO and external auditor; cross-border transfers are generally allowed. As a general rule, it is prohibited to process genetic, biometric, health data, or data relating to ethnic origin, sexuality, political or religious opinions, beliefs, criminal convictions, or security measures without a permit from the authority. Violators will face fines of up to $1.3 million for noncompliance.

The Kingdom of Bahrain

The Personal Data Protection Law has been in force since August 1, 2019 and includes a variety of liabilities for violations, including the withdrawal of the DPA's authorization, publication of statement of violation, suspension of data processing, fines (of up to $53,000), or imprisonment. The law includes extraterritorial reach to those individuals or entities located in Bahrain and those processing personal data using means in Bahrain, regardless of their place of residence.

By default, the appointment of the DPO is not required. Additionally, a data breach must be notified within 72 hours, and cross-border data transfers are generally prohibited unless expressly allowed by law or when the transfer is necessary for execution of a contract with a first party for the benefit of a data subject.

The State of Qatar

The State of Qatar has its own regulations that are separate and distinct from the Qatar Financial Centre (QFC). The State of Qatar's Data Protection Law came into force in 2016 and was the first GCC member state to issue a generally applicable data protection law. The Data Protection Office, an independent institution of the QFC, administered the QFC Data Protection Regulations, which came into force on June 19, 2022. Both laws carry significant fines and restrictions, with enforcement actions continuing to be developed. Other issues of note: the appointment of the DPO is not mandatory, but processing of data related to children, criminal activities, health, ethnicity, religion, and marital relations requires the DPA's permit.

According to the general data protection framework, it is a data controller's obligation to provide information on processing before it starts. Data controllers must create a personal data management system and are subject to data breach notification requirements within 72 hours.

The State of Kuwait

The Data Privacy Protection Regulation has been in force since April 4, 2021, and its extraterritorial reach applies to persons providing communication and information technology services and operating websites, smart applications, or cloud computing services targeting users in Kuwait (service providers). A service provider must notify the user of all information and service conditions in both English and Arabic, including on the alleged cross-border transfer of the data. Cross-border data transfers are subject to a four-tier classification system, with data categorized in tier 3 and tier 4 being unable to be transferred outside of Kuwait.

Learn More

In our recent Technology Marathon presentation Privacy in the Middle East, we discuss what companies should consider when doing business in the UAE, Saudi Arabia, Oman, Kuwait, and Qatar.

CONCLUSION

As regulations evolve, responding to changes has been of paramount concern for multinational corporations. Businesses should consider the following to remain compliant:

- Conduct a security self-assessment and personal information protection impact assessment;
- Prepare data transfer agreements; and
- Review and update current data-related policies, as well as both internal employee notices and external-facing privacy notices and policies.

Subscribe to receive Morgan Lewis publications for updates on trends, legal developments, and hot topics in global data privacy laws and other relevant areas.

AUTHORS

If you have any questions or would like more information on the issues discussed in this report, please contact any of the following:

Philadelphia

Ezra D. Church	+1.215.963.5710	ezra.church@morganlewis.com
Kristin M. Hadgis	+1.215.963.5563	kristin.hadgis@morganlewis.com
Gregory T. Parks	+1.215.963.5170	gregory.parks@morganlewis.com
Terese M. Schireson	+1.215.963.4830	terese.schireson@morganlewis.com

San Francisco

W. Reece Hirsch	+1.415.442.1422	reece.hirsch@morganlewis.com

Washington, DC

Ronald W. Del Sesto, Jr.	+202.739.6023	ronald.delsesto@morganlewis.com

London

William Mallin	+44.20.3201.5374	william.mallin@morganlewis.com

Shanghai

Todd Liao	+86.21.8022.8799	todd.liao@morganlewis.com
Sylvia Hu	+86.21.8022.8527	sylvia.hu@morganlewis.com

Dubai

Ksenia Andreeva	+971.4.312.1865	ksenia.andreeva@morganlewis.com
Alena Neskoromyuk	+971.4.312.1856	alena.neskoromyuk@morganlewis.com

ABOUT US

Morgan Lewis is recognized for exceptional client service, legal innovation, and commitment to its communities. Our global depth reaches across North America, Asia, Europe, and the Middle East with the collaboration of more than 2,200 lawyers and specialists who provide elite legal services across industry sectors for multinational corporations to startups around the world. For more information about us, please visit www.morganlewis.com.

Morgan Lewis

At Morgan Lewis, we're always ready to respond to the needs of our clients and craft powerful solutions for them.

Connect with us

www.morganlewis.com

080723_232067