Morgan Lewis

REPORT

GLOBAL PRIVACY

YEAR IN REVIEW AND A LOOK FORWARD

2023-2024

www.morganlewis.com

Morgan Lewis

GLOBAL PRIVACY: YEAR IN REVIEW AND A LOOK FORWARD 2023–2024

TABLE OF CONTENTS

GLOBAL PRIVACY: YEAR IN REVIEW AND A LOOK FORWARD 2023–2024

The world is witnessing a flurry of activity surrounding issues of data protection, cybersecurity, artificial intelligence (AI), and consumer privacy.

According to the National Conference of State Legislators, some 40 US states have introduced or are currently considering legislation to govern relevant data. Following California's lead in enacting comprehensive consumer privacy legislation in 2018, 13 states have passed similar privacy laws. For 2023 in particular, privacy was a lead story when it came to consumer litigation, with plaintiffs filing a wave of lawsuits that will test the scope of older wiretap and other privacy laws as applied to the internet.

During the same year, the European Union saw significant legislative activity with respect to online content moderation obligations, cybersecurity, and AI. The United Kingdom too was active with respect to online content moderation. Data protection regulators in the EU brought regulatory enforcement actions relating to the EU General Data Protection Regulation (GDPR), while the UK data protection regulator defended appeals brought against UK GDPR enforcement actions brought in prior years.

Privacy-related legislative activity was also robust in Asia, with comprehensive privacy legislation coming into full effect in China and new privacy legislation being enacted in India. In the Middle East, we saw developments from several regional players, including the Hashemite Kingdom of Jordan and the Kingdom of Saudi Arabia around personal data handling and requirements for predictive and prescriptive AI systems.

Looking back over global privacy developments 2023, there's clearly a lot to talk about— in this report we identify some of the key highlights as well as our predictions for the rest of 2024.

2023 HIGHLIGHTS

UNITED STATES

New Consumer Privacy Protections Implemented

We saw several new consumer privacy laws go into effect in 2023, including significant revisions to the California Consumer Privacy Act (CCPA) and new comprehensive privacy laws in Colorado, Connecticut, Utah, and Virginia. More change is coming as a flurry of new consumer privacy laws enacted over the course of 2023, including in Delaware, Indiana, Iowa, Montana, Oregon, Tennessee, and Texas, will go into effect over the next three years, and several other states are debating privacy legislation of their own. In fact, the first privacy law of 2024 has already been enacted in New Jersey. Assessing their similarities and differences is vital to planning and executing a compliance strategy for companies operating in multiple states.

Learn more >

Illinois Supreme Court Held Healthcare Employee Fingerprint Data Is Exempt from Biometric Information Privacy Act

In the first win for defendants facing Illinois Biometric Information Privacy Act (BIPA) litigation before the Illinois Supreme Court, in December 2023, the court in *Mosby v. Ingalls Memorial Hospital* held that BIPA

excludes from its protections the biometric information of healthcare workers where that information is collected, used, or stored for healthcare treatment, payment, or operations.

Learn more >

California Enacted the Delete Act

In October, California enacted its newest privacy legislation, commonly referred to as the Delete Act (California Senate Bill No. 362). The Delete Act will allow any consumer to request that any data broker that maintains any personal information related to that consumer delete such personal information.

Businesses that knowingly collect and sell to third parties the personal information of a consumer with whom the business does not have a direct relationship should pay close attention to the definition of "data broker." If the business determines that it is a data broker, it should ensure that it complies with the requirements of the Delete Act, including the obligation to register, in order to avoid penalties. Data brokers will need to develop and maintain internal policies to review consumer deletion requests to comply with the Delete Act's deletion timelines, be prepared for the volume of deletion requests, implement policies to verify deletion requests, maintain records for audit obligations, track the type of data they collect (including personal information such as information of minors, precise geolocation, or reproductive healthcare data), and keep updated privacy policies.

The Delete Act will also impact businesses that obtain consumer data from data brokers, as such data may not be permanently available if a consumer asks a data broker to delete their data. A business that has relied on such data for verification purposes, for example, will need to be prepared to find alternate ways to verify consumer information.

Learn more >

Federal Trade Commission Amended the Safeguards Rule

In October 2023, the Federal Trade Commission (FTC) adopted a final rule amending its Standards for Safeguarding Customer Information (commonly referred to as the Safeguards Rule) to require financial institutions to report certain data breaches and other security events to the FTC. The final rule requires financial institutions to report notification events, defined as the unauthorized acquisition of unencrypted customer information, involving at least 500 customers to the FTC within 30 days after discovery of the notification event.

With the approaching May 2024 deadline for the Safeguards Rule, all financial institutions subject to these requirements should review and, if necessary, update their policies and procedures to be in a position to comply with these new federal data breach reporting requirements.

Learn more >

Federal Trade Commission Proposed Expanding the Negative Option Rule

Last spring, the FTC, in a 3-1 vote with Commissioner Christine S. Wilson (R) dissenting, published a notice of proposed rulemaking regarding an amendment to the FTC's Negative Option Rule concerning subscription services. The proposed rule would significantly increase enforcement risk and require redesign and coding changes with compliance and legal review by skilled technicians and lawyers. The financial risks of noncompliance are significant.

FTC rules are often interpreted by state attorneys general as violations of state law and are enforced in state courts under state law under legally unfavorable circumstances. After receiving comment, the FTC

published the new proposed Negative Option Rule in the *Federal Register* on December 4, 2023, and an informal hearing was scheduled for January 16.

Learn more >

New Federal Cybersecurity Requirements Were Released

Also in the spring, US regulators increased their focus on cybersecurity issues impacting financial services companies, with a host of guidance documents released by the US Securities and Exchange Commission (SEC); the three federal banking agencies: the Federal Reserve Board, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency; and the US Department of Labor (DOL). Often targeted for its data and money, the financial sector's rapid digitalization has led to an increase in global cyber threats.

Financial institutions should consider reviewing their policies, procedures, and contracts with service providers to ensure compliance with these new federal requirements.

Learn more >

Washington Governor Signed the My Health My Data Act

This spring and summer, The My Health My Data Act, signed by the governor of Washington State last April, takes effect and is expected to have an impact on the privacy practices of a wide range of digital health businesses—potentially reaching beyond the state's borders. While the act is effective on March 31, 2024 for regulated entities and on June 30, 2024 for small businesses, the act's geofencing provision became effective on July 23, 2023.

The legislature described the act as a "gap-filler," intended to protect consumer health data not otherwise protected by state and federal healthcare privacy regulations, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Washington's Uniform Health Care Information Act (UHCIA), and 42 CFR Part 2 (regulating patient substance use disorder records). Despite significant carveouts, the act has wide-reaching privacy implications for Washington and non-Washington consumers and businesses and will likely spur numerous class action and similar legal challenges for regulated entities.

Learn more >

Securities and Exchange Commission Adopted Mandatory Cybersecurity Disclosure Rule

In July, the SEC adopted final rules and amendments for mandating disclosure regarding cybersecurity risk management, strategy, governance, and incident reporting, including amendments to Forms 8-K, 6-K, 10-K, and 20-F. Under the new framework, public companies must report certain details of a cybersecurity incident within four days of determining such an incident is material and provide certain expanded standardized cybersecurity-related disclosures and assessments in annual reports. The final rule formalizes the SEC's efforts to address its concerns regarding information asymmetry and under-disclosure around the cause, scope, impact, and materiality of cybersecurity incidents.

In light of the final rule and the SEC's increased focus on cybersecurity risk management generally, it is important for companies to take proactive steps now to address cybersecurity issues in anticipation of these new disclosure requirements.

Learn more >

California Enforced Consumer Privacy Law with an 'Investigative Sweep'

In a nod to Data Privacy Day, California Attorney General Rob Bonta announced an "investigative sweep" directed primarily at ensuring that businesses can accept and timely process consumer opt-out requests. Although not limited in scope, the attorney general (AG) noted an emphasis on retail, travel, and food services businesses in this wave of enforcement. As with the existing right to opt out of the sale of personal information, businesses must present consumers with a straightforward way to submit these requests, and they must also be processed within 15 business days.

Given the AG's enforcement push, it is critical that covered businesses in California have an efficient and functioning system for receiving and processing opt-out requests. In the wake of recent settlements of claims by the AG resolving allegations that companies failed to process CCPA opt-out requests, this investigative sweep demonstrates that the AG intends to actively enforce the landmark privacy law.

Learn more >

Plaintiffs Advanced a Novel Theory on the Video Privacy Protection Act

The Video Privacy Protection Act (VPPA) "creates a private right of action for plaintiffs to sue persons who disclose information about [consumers'] video-watching habits." In 2023, plaintiffs bringing suits under the VPPA advanced a new and novel theory of VPPA liability by claiming that a company violates the act when a consumer clicks on a video on the company's site and the company then sends their data to a third party that operates the tracking technology—for example, when a person watches a video on a retailer's site, and the retailer uses a third-party pixel to track the individual's use.

Enacted in 1988, the VPPA was originally intended to prevent the wrongful disclosure of rental and sale records of "video cassette tapes or other similar audio visual materials." Plaintiffs are now seeking to further expand the reach of the VPPA online. The VPPA allows recovery of $2,500 in statutory damages for violations, which, if applied to a broad class, can create significant exposure.

UK AND EUROPE

Council of the European Union Adopted the Data Act

The Council of the European Union adopted the Data Act on November 27, 2023. The Data Act, together with the Data Governance Act and EU GDPR as key elements of the broader European data strategy, aim to create a unified market for the free flow of data within the EU and across various sectors as well as to address data flows of nonpersonal data from the EU to countries outside of the EU differently from the GDPR, which continues to cover personal data. This pivotal legislation took effect January 11, 2024.

Learn more >

EU-US Data Privacy Framework Took Effect Following Extension

The EU-US Data Privacy Framework (DPF) became effective on July 10, 2023 and that 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 (DOT) are eligible to self-certify their compliance with the DPF.

The introduction of the EU-US DPF Program establishes a foundation for a streamlined approach to transfers of personal data from the European Union to the United States. All organizations interested in transferring EU personal data to the United States need to carefully assess their eligibility, adhere to the

DPF principles, and ensure compliance with relevant US laws and the GDPR as applicable. Transfer of personal data from the UK is also possible through the UK-US Data Bridge.

Learn more >

NIS 2 Directive Entered Into Force

The NIS 2 Directive (Directive), which establishes unified legal measures aiming to boost cybersecurity in the EU, entered into force on January 16, 2023; EU member states must transpose it into national law by October 17, 2024. The Directive requires EU countries to adopt a national cybersecurity strategy that "provides for the strategic objectives, the resources required to achieve those objectives, and appropriate policy and regulatory measures, with a view to achieving and maintaining a high level of cybersecurity" (Article 7, NIS 2 Directive).

Member states must designate competent authorities and a single point of contact to supervise the cybersecurity requirement (Article 8, NIS 2 Directive), and for the management of largescale cybersecurity incidents and crises (Article 9, NIS 2 Directive). Furthermore, to strengthen the reporting obligations, each member state shall designate or establish one or more computer security incident response teams (Articles 10 to 12, NIS 2 Directive). Finally, the NIS 2 Directive coordinates the dynamics of cooperation on both the member state level (Article 13, NIS 2 Directive) and the EU level (Articles 14 to 18, NIS 2 Directive).

Europe Took the Lead on Comprehensive AI Regulation

After lengthy negotiations, representatives of the EU Council, European Parliament, and European Commission reached a compromise in principle last year on rules for the use of AI, ushering in new safeguards, consumer rights, product liability, and fines, among many other components. The AI Act appears poised for final approval this year and will be implemented in stages in the next few years.

Learn more >

European Court of Justice Facilitated Access to Vehicle Data for Independent Vehicle Repairers

In two recent judgments, the European Court of Justice (ECJ) mandated information access rights by independent vehicle repairers to vehicle data under Regulation (EU) 2018/858. The judgments are likely to facilitate access to vehicle data to independent vehicle repairers.

Vehicle manufacturers will need to consider the implications of this regulation and these judgments as early as possible in designing their vehicles. Notably, there is a potential tension between this data sharing requirement and other legal obligations that may apply to vehicle manufacturers; for example, an obligation to incorporate robust cybersecurity measures in the vehicle's design or any data protection obligations arising from the EU GDPR.

Learn more >

For more information on 2023 privacy law developments in the UK and EU, read our *Law360* Expert Analysis >

ASIA AND THE MIDDLE EAST

Beijing Courts Found That WeChat Records Recovered Without Employee Consent Were Inadmissible

A Beijing appellate court rejected an employer's ability to use—without the employee's informed consent—deleted WeChat data from a company-issued device in a legal proceeding to support the termination of an employee's employment contract by demonstrating misconduct. The Beijing appellate court's view is likely to be followed more broadly, so employers should adjust data protection policies and consents to reflect broader forms of personal data that the company may collect.

Learn more >

China Passed New Anti-Espionage Law

On April 26, 2023, the Second Session of the Standing Committee of the 14th National People's Congress voted and passed the revised Anti-Espionage Law of the People's Republic of China (the New Anti-Espionage Law). The New Anti-Espionage Law, which took effect on July 1, 2023, expands the scope of espionage activities, establishes broad criteria for determining espionage behavior, grants extensive investigative power to national security agencies, and clarifies the legal liability for espionage activities.

Learn more >

China Issued Its SCC Template and Governing Regulation

China issued the standard contractual clause (SCC) template and its governing regulation (the SCC Measures), effective June 1, 2023. An SCC is an agreement between the data handler and the recipient relating to the handling, storage, and deletion of data, among other areas, under the context of cross-border transfers of personal information. The China SCC template contains certain similar requirements to those under the EU GDPR.

The standard terms of the SCC cannot be changed, and supplemental provisions are only permissible if they do not conflict with the standard terms. There was a six-month grace period, with a deadline of November 30, 2023, for data handlers engaging in cross-border data transfer activities—which are not subject to a security assessment—to comply with the requirements under the SCC Measures and/or the Personal Information Protection Law for past data transfer activities.

Learn more >

China Issued First SCC Filing Guidelines for Cross-Border Transfer of Personal Information

On May 30, 2023, China's national Cyberspace Administration of China (CAC) released the long-awaited Guidelines for Filing Standard Contracts for the Cross-border Transfer of Personal Information (First Edition) (SCC Filing Guidelines). This development was important because it pertains to the lawful transfer of personal information outside of China.

The national CAC previously issued regulations requiring personal information handlers to go through one of the three regulatory pathways before they are allowed to lawfully transfer personal information to overseas recipients: (1) for certain data exporters who are considered critical information infrastructure operators (CIIOs), who handle "important data," or who export personal information meeting certain volume thresholds, they should pass a CAC-led security assessment; (2) for those not meeting the above thresholds, they should either (a) sign a CAC-issued standard contract template with overseas data

recipients, or (b) pass a data security certification administered by a qualified certification agency. The deadline to comply with the SCC pathways for the past data transfer activities was November 30, 2023.

The SCC Filing Guidelines provide specific requirements for filing methods, procedures, and required documentation under the SCC pathways, which helps streamline and facilitate the filing process. It also included the long-awaited template for the Personal Information Protection Impact Assessment Report (PIPIA Report). The PIPIA Report is part of the required filing documentation to be produced by the personal information handler, which aims to internally assess the impact of the data export activity by addressing its legality, legitimacy, and necessity; the risks to personal information rights; the security measures and capabilities of the overseas data recipient; the risks of data tampering, destruction, leakage, loss, or unauthorized use; the availability of channels for protecting personal information rights; and the impact of the recipient's country or region's personal information protection policies and regulations on the implementation of SCCs.

China Published Exposure Draft to Regulate and Promote Cross-Border Data Flow

On September 28, 2023, China's national CAC published the Exposure Draft of Regulations to Regulate and Promote Cross-Border Data Flow (the Exposure Draft), which intends to substantially alleviate the compliance burden on general companies for cross-border data transfer.

According to the Exposure Draft, for the following cross-border data transfer scenarios, the company is not required to apply for the CAC-led security assessment, sign the SCCs, or pass the personal information protection certification (Certification):

1. It is necessary to provide personal information abroad for the purpose of concluding and performing contracts to which the individual is a party, such as cross-border shopping, cross-border fund remittance, air ticket and hotel booking, and visa handling.
2. It is necessary to provide the internal employees' personal information abroad for human resource management purposes according to the labor rules and regulations or the collective contracts made or signed in accordance with PRC laws and regulations.
3. It is necessary to provide personal information abroad to protect the life, health, and property etc. of natural persons in case of emergency.

Further, the Exposure Draft provided the following scenarios:

1. If it is anticipated that within one year the company will cross-border transfer no more than 10,000 individuals' personal information, the company does not need to conduct the CAC-led security assessment, sign the SCCs, or pass the Certification.
2. If it is anticipated that within one year the company will cross-border transfer more than 10,000 but fewer than 1 million individuals' personal information, the company does not need to conduct the CAC-led security assessment but does need to sign the SCCs and make the SCC filing with the local CAC.
3. If it is anticipated that within one year the company will cross-border transfer more than 1 million individuals' personal information, it still needs to apply for the CAC-led security assessment.

The Exposure Draft emphasizes the consent requirement: if the company provides personal information abroad based on the individuals' consent, the company shall still obtain the individual's consent.

For Free Trading Zones (FTZ), according to the Exposure Draft, the FTZ has the autonomy to make a negative data list (the Negative List). If the company transfers data that does not fall under the Negative List abroad, it does not need to apply for the CAC-led security assessment, sign the SCC, or pass the Certification.

China Issued Detailed Implementation Rules for Management of Human Genetic Resources

On June 1, 2023, China's Ministry of Science and Technology (MOST) officially announced the release of the "Detailed Implementation Rules for the Management Regulations of Human Genetic Resources" (the Detailed HGR Rules). These rules, which took effect on July 1, 2023, represent a significant milestone in the regulation of human genetic resources (HGR) in China. The Detailed HGR Rules, which build upon the earlier draft version issued by MOST on March 21, 2022, provided comprehensive guidance and operational details for the management of HGR. They address various concerns and issues that have emerged since the implementation of the Regulations on the Management of Human Genetic Resources (HGR Regulations) in 2019.

Learn more >

China Released Government Notice on Automotive 'Important Data' Disclosure

In late November and early December 2023, China's local CACs (e.g., Guangdong CAC, Zhejiang CAC, Beijing CAC, and Shanghai CAC) released the government notice on automotive "important data" filings, which required local automotive data handlers to disclose their data processing activities to the relevant CAC before December 15. The granularity of the disclosure could be very detailed.

According to the Guangdong CAC's template, automotive data handlers needed to disclose the total volume of automotive data obtained in 2023, the categories of such automotive data, the necessity of handling it, and the cross-border transfer details. According to the Provisions on Automotive Data Security Management (for Trial Implementation) published in 2021, an automotive data filing is required annually.

China Established a National Data Bureau

China's National Data Bureau was established on October 25, 2023. According to the China State Council's official description, the National Data Bureau is responsible for advancing the development of data-related fundamental institutions; coordinating the integration, sharing, development, and application of data resources; and pushing forward the planning and building of a digital China, the digital economy, and a digital society, among others.

China Issued Exposure Draft on Compliance Audits for Personal Information Protection

On August 3, 2023, China issued the Exposure Draft Administrative Measures of Compliance Audit on Personal Information Protection (the Exposure Draft for Personal Information Audit).

According to the Exposure Draft for Personal Information Audit, a personal information handler that handles the personal information of more than 1 million individuals shall carry out the compliance audit of personal information protection at least once a year, and any other personal information handler shall conduct the compliance audit of personal information protection at least once every two years.

The Exposure Draft for Personal Information Audit also provides that where a personal information handler carries out the compliance audit of personal information protection by itself, it may mandate an internal body within the organization or entrust a specialized agency to carry out such audit as required by these measures in light of the actual conditions.

The key aspects of the personal information audit are comprehensive, including but not limited to the legal basis for the personal information handler to handle the personal information, the personal information-handling rules, the informed consent, the channels for the personal information subject to exercise their personal information rights, the related company structure, and policies and standard operating procedures. The Exposure Draft for Personal Information Audit also provides detailed rules for specific personal information-handling scenarios.

India Enacted the Digital Personal Data Protection Act

India enacted its new privacy law—the Digital Personal Data Protection Act, 2023 (DPDP Act)—on August 11, 2023. Once in effect, the DPDP Act will replace the relevant provisions of the Information Technology Act, 2000; Information Technology (Amendment) Act, 2008; and Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. The law will come into effect on a date to be decided by the central government, which is authorized to determine different dates for entry into force of various provisions of the legislation. The central government is also entitled to enact separate rules to give effect to various provisions of the DPDP Act.

Only when these rules are issued will we be able to understand the full scope of this new law. In the interim period, businesses should ensure that their data systems and practices continue to comply with the provisions of current laws.

Learn more >

DIFC Introduced New Requirements on Processing of Personal Data via AI, Similar Tools

The Dubai International Financial Centre (DIFC), a global financial center in Dubai, United Arab Emirates, introduced revisions to its data protection law (the DIFC DPL) that establish a rather complex set of obligations for users and operators of autonomous and semi-autonomous systems. The new requirements affect a wide array of systems, including predictive and prescriptive AI systems and generative machine-learning (ML) technology, that require minimal human input.

Unlike the approach taken in many other jurisdictions, the position of the DIFC is to avoid regulation of the content of algorithms directly. Instead, the law sets boundaries for companies deploying, operating, or providing AI systems in terms of their processing of personal data. Interestingly, the scope of affected personal data may extend to the identification of virtual personas or similar virtual identifiers used to represent individuals, such as personas created for the metaverse.

ADGM Office of Data Protection Published Addendum to EU Standard Contractual Clauses

Another financial center of the UAE, the Abu Dhabi Global Market (ADGM), has its own Office of Data Protection that diligently tracks global trends in privacy and data protection and implements them to support ADGM businesses. The Office of Data Protection has been discussing the necessity of providing additional support to ADGM businesses engaged in cross-border data transfers involving individuals' personal data for quite some time. The long-awaited work resulted in the publication of an addendum to the European Commission's SCCs for the transfer of personal data.

Given the number of restrictions on cross-border transfers without adequate safeguards that are introduced not only in the EU but in other jurisdictions too, it is expected that with this addendum, ADGM businesses will streamline processes, reduce duplication, and alleviate additional compliance burdens, especially when working with EU counterparties.

Kingdom of Saudi Arabia Issued New Personal Data Protection Law and Implementing Regulations

The initial text of the Kingdom of Saudi Arabia (KSA) Personal Data Protection Law (KSA PDPL) was approved in 2021 and supposed to come into force in March 2023. However, substantial amendments were rather unexpectedly made to the initial draft in 2023. These amendments were partly in response to feedback from the KSA business community, who objected to the overly strict regulations proposed for handling personal data collected in the KSA. (Initially, consent was to be the primary legal basis for data processing, and cross-border data transfers necessitated approval from the Saudi data protection authority.)

The revised KSA PDPL took effect on September 14, 2023, offering businesses operating in or handling data related to the KSA a one-year transition period to bring their data processing activities and practices in line with the KSA PDPL requirements. Enforcement of the KSA PDPL is anticipated to begin on or after September 14, 2024.

Right before the KSA PDPL came into force in September, its Implementing Regulations were published and were found to provide lacking details as to the KSA PDPL and, in some cases, to elucidate the legislative intent behind certain provisions. The Implementing Regulations elaborated on several key concepts introduced by the KSA PDPL, such as the concept of legitimate interest as a legal basis for data processing and criteria for cross-border data transfers' adequacy, among others. However, as of now, the Implementing Regulations have not provided all the necessary rules and details, and the KSA business community anticipates further guidance and directives from the regulator in the near future.

The regulatory authority responsible for data protection in the KSA is the Saudi Data & AI Authority (SDAIA), comprising three divisions overseeing data protection, AI, and national information. These divisions are the National Information Center, National Center for AI, and National Data Management Office (NDMO). In its turn, the NDMO serves as the legislative arm of the SDAIA, developing and implementing plans, policies, data regulations, and programs; overseeing compliance; and performing functions akin to those of data protection offices in other jurisdictions. Actively engaging with the business community, the NDMO regularly disseminates newsletters outlining its positions on technology, AI, and data topics, and fosters direct dialogue with both national and global businesses operating in the KSA.

Jordan Issued Personal Data Protection Law

The Hashemite Kingdom of Jordan has introduced comprehensive national legislation to govern the collection and handling of personal data. The Jordan Personal Data Protection Law No. 24 of 2023 (Jordanian PDPL) concerning personal data protection was enacted almost simultaneously with the new Jordanian Electronic Crimes Law, which defined various cybercrime offenses.

The Jordanian PDPL will become effective March 17, 2024 and will have retrospective application to the processing of data collected prior to its enactment. The law allows a one-year grace period to align with the new legal requirements.

Similar to other international legislation, the Jordanian PDPL applies to the processing of personal data or sensitive personal data and distinguishes between the roles and responsibilities of controllers and

processors handling data on behalf of controllers. Interestingly, the Jordanian PDPL does not specify its geographic scope or extraterritorial application.

2024 PREDICTIONS

UNITED STATES

- We will continue to see states follow California in enacting state privacy laws; we will also be looking to see if any states deviate from California or other states in material ways.
- Court decisions will provide some guidance to companies grappling with how wiretap statutes may apply to online tracking technologies.
- AI regulation will be a hot topic in Congress, but—as with privacy—we expect that states and cities will be the first jurisdictions to regulate AI.
- We expect increased SEC enforcement and related activity around the new cybersecurity disclosure rules.

UK AND EUROPE

- GDPR enforcement: EU/UK GDPR regulators will continue to focus their enforcement efforts on children's online data protection and key GDPR basics, namely transparency and lawfulness.
- AI: We predict the new EU AI Act will be agreed. GDPR enforcement action will expand regarding generative AI. Developers and users of AI/ML technologies will grapple with the European Court of Justice's SCHUFA decision applying the EU GDPR.
- Data transfers: EU/UK data protection regulators will focus on data transfers to the People's Republic of China now that the EU-US Data Privacy Framework and UK-US Data Bridge have been agreed.
- Digital Services Act (DSA) and UK Online Safety Act: The European Commission will begin to enforce the DSA's content moderation rules.
- Cybersecurity: Organizations covered by the EU NIS 2 Directive will initiate compliance readiness programs relative to statutory cybersecurity obligations applicable to them.

ASIA

- Cross-border data transfer burdens could be eased when the Exposure Draft of China's Regulations to Regulate and Promote Cross-Border Data Flow is finalized.
- Important data processors could be required to file to the authorities, similar to the current filing requirement for the automotive industry.

MIDDLE EAST

- The highly anticipated publication of the Implementing Regulations to the UAE Privacy Law (Federal Decree Law No. 45/2021) in 2024 is expected to provide clarification on several aspects of the law, including its scope and the severity of penalties.
- We will monitor the application of DIFC guidance on international personal data transfers.
- Companies operating in the DIFC and engaged in the development of AI systems and ML models (as well as those considering the use of AI/ML for their operations) should ensure that they comply with the requirements set out in the new DIFC law to avoid severe penalties.
- It is yet to be determined how the data protection authority in the KSA will implement the KSA PDPL requirements and how the business community will respond to them.
- It remains to be seen how the interpretation and enforcement of the Jordanian PDPL will evolve.

CONCLUSION

It is clear that 2023 saw an extraordinarily intense round of privacy legislation, regulation, and litigation, and 2024 promises to expand on that trend. We are likely to see more states follow California in enacting privacy laws, including New Jersey, which was the first state to enact legislation in the new year. Courts will provide guidance on the likes of online tracking technologies, biometrics, and other new ways in which personal information is collected and used. The use of AI and its many implications for the blurring of public-private borders will occupy Congress, state legislatures, and governments worldwide.

The EU and UK will surely continue to take the lead on regulation, particularly when it comes to AI. Those jurisdictions, as well as China and India, will be scrutinizing cross-border data transfers. Asian nations are also likely to increase requirements for data processors to report to authorities.

While the particulars might vary across geographies, in the coming year companies will have to be even more vigilant about central principles such as transparency and compliance.

CONTACTS

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
Kathryn E. Deal	+1.215.963.5548	kathryn.deal@morganlewis.com
Terese M. Schireson	+1.215.963.4830	terese.schireson@morganlewis.com
Emily Wheeling	+1.215.963.5876	emily.wheeling@morganlewis.com
Julian Williams	+1.215.963.5359	julian.williams@morganlewis.com

Princeton

Gregory T. Parks	+1.609.919.6681	gregory.parks@morganlewis.com

London

Vishnu Shankar	+44.20.3201.5558	vishnu.shankar@morganlewis.com
William Mallin	+44.20.3201.5374	william.mallin@morganlewis.com

Chicago

Elizabeth B. Herrington	+1.312.324.1445	beth.herrington@morganlewis.com

San Francisco

W. Reece Hirsch	+1.415.442.1422	reece.hirsch@morganlewis.com
Carla B. Oakley	+1.415.442.1301	carla.oakley@morganlewis.com
Phillip Wiese	+1.415.442.1483	phillip.wiese@morganlewis.com
Ali Gonsman	+1.415.442.1159	alexandra.gonsman@morganlewis.com
Kevin M. Benedicto	+1.415.442.1340	kevin.benedicto@morganlewis.com

Houston

Catherine North Hounfodji	+1.713.890.5120	catherine.hounfodji@morganlewis.com
Sydney Reed Swanson	+1.713.890.5105	sydney.swanson@morganlewis.com

Paris
Charles Dauthier +33.1.53.30.44.74 charles.dauthier@morganlewis.com

Washington, DC
Ronald W. Del Sesto, Jr. +1.202.739.6023 ronald.delsesto@morganlewis.com
Dr. Axel Spies +1.202.739.6145 axel.spies@morganlewis.com

Dubai
Ksenia Andreeva +971.4.312.1865 ksenia.andreeva@morganlewis.com

Shanghai
Todd Liao +86.21.8022.8799 todd.liao@morganlewis.com

Seattle
Amy M. Magnano +1.206.274.6451 amy.magnano@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.

www.morganlewis.com