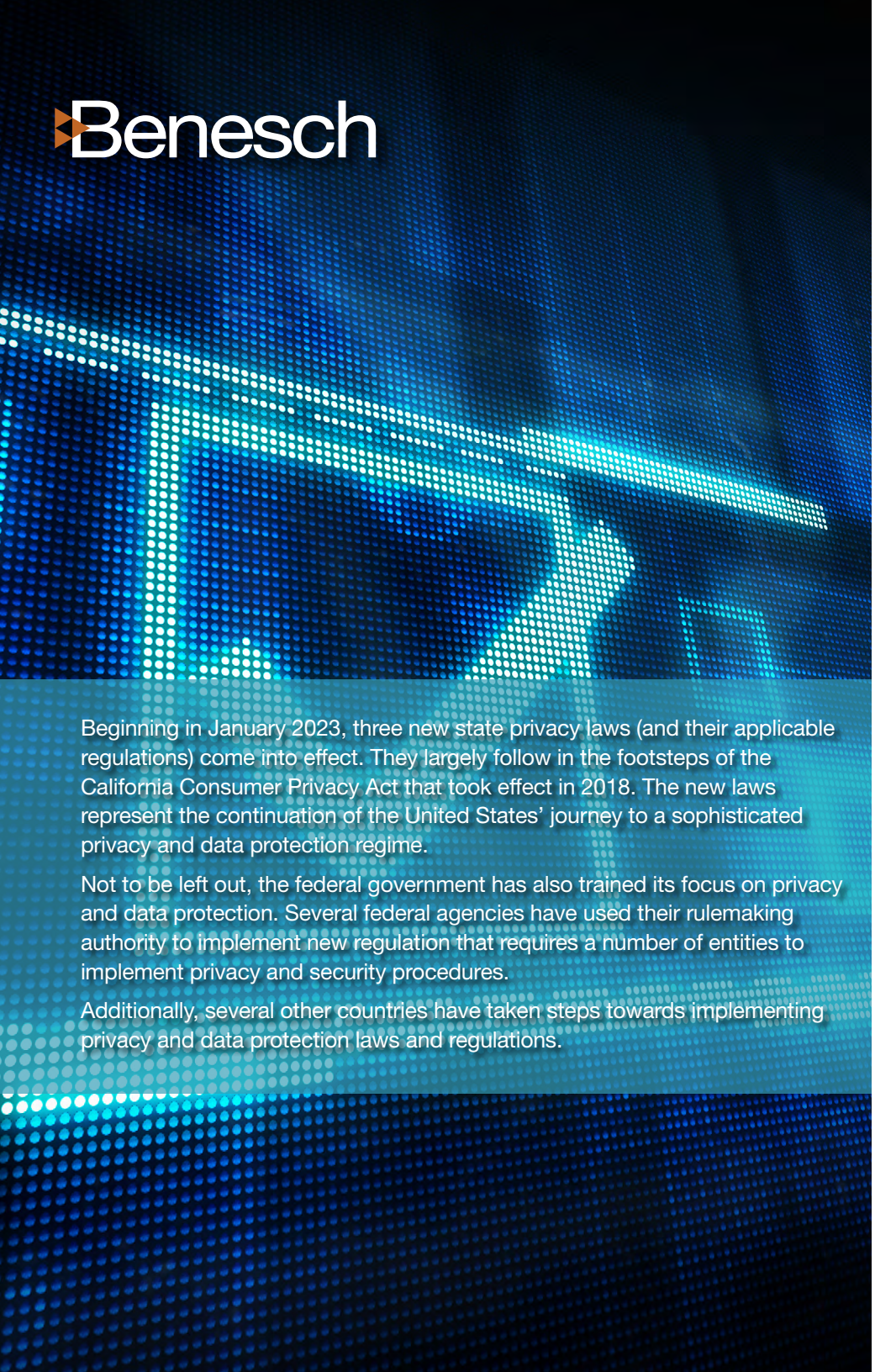

Beginning in January 2023, three new state privacy laws (and their applicable regulations) come into effect. They largely follow in the footsteps of the California Consumer Privacy Act that took effect in 2018. The new laws represent the continuation of the United States' journey to a sophisticated privacy and data protection regime.

Not to be left out, the federal government has also trained its focus on privacy and data protection. Several federal agencies have used their rulemaking authority to implement new regulation that requires a number of entities to implement privacy and security procedures.

Additionally, several other countries have taken steps towards implementing privacy and data protection laws and regulations.

2022 Data Protection & Privacy TO-DO LIST

STATE LAWS

New state privacy laws come into effect in 2023 in California, Colorado, and Virginia. The three new privacy and data protection laws build on the momentum that the California Consumer Privacy Act started—one of the new law's amends the existing California law—and marks a continuation of separate states continuing to try and address consumer privacy and data protection concerns. The federal government, while taking action on the cybersecurity front, has largely shied away from taking action on omnibus privacy and data regulation. This has left the states to take California's lead in passing their own.

For an in-depth look at the various nuances and requirements under the three new state laws, please check out the Data Meets World website.

California

In 2020, California privacy interest groups were successful in getting a privacy referendum on the November ballot. The referendum consisted of overhauling and amending the existing California Consumer Privacy Act. On November 3, 2020, California voters approved of the California Privacy Rights Act with over 56% of voters supporting the measure. The California Privacy Rights Act takes effect on January 1, 2023.

The main changes under the new law include: (1) the categorization and regulation of sensitive personal information; (2) the right for an individual to limit a business's use of sensitive personal information; (3) data minimization standards; (4) restrictions on the use of cookies for cross-contextual behavioral advertising; (5) annual cybersecurity review and audit requirements; (6) the creation of the California Privacy Protection Agency; and (7) the expansion of a limited private right of action.

Colorado

In July of 2021, the governor of Colorado officially signed the Colorado Privacy Act into law. The Colorado Privacy Act largely sets up a dynamic similar to Europe's GDPR where there are Controllers and Processors of personal information. Additionally, the new Colorado law is very similar in substance to the Virginia law below. The Colorado Privacy Act takes effect on January 1, 2023.

The main provisions include: (1) individual rights, including the right to access, correction, and deletion; (2) the implementation of a "controller" and "processor" regime; (3) contractual standards and floors that must be meet in controller and processor relationships; (4) opt-in consent

requirements for the collection and processing of Sensitive Data; (5) risk assessment and audit requirements; and (6) individual opt-out rights for the selling of personal information, targeted advertising, and profiling in furtherance of legal (or similar) decisions.

Virginia

In March of 2021 the governor of Virginia signed the Consumer Data Protection Act into law, making it only the second state at the time to have passed a comprehensive privacy and data protection law. Similar to the GDPR in Europe, the new Virginia law sets up a Controllers and Processors dynamic. Additionally, the new Virginia law is very similar in substance to the Colorado law above, which was passed after the Virginia law. The Consumer Data Protection Act takes effect on January 1, 2023.

The main provisions of the new law include: (1) individual rights, including the right to access, correction, and deletion; (2) the implementation of a "controller" and "processor" regime; (3) contractual standards and floors that must be meet in controller and processor relationships; (4) opt-in consent requirements for the collection and processing of Sensitive Data; (5) risk assessment and audit requirements; and (6) individual opt-out rights from the selling of personal information, targeted advertising, and profiling in furtherance of legal (or similar) decisions.

State Law To-Do List

- ☐ **Drafting internal and external policies:** Notice to the individual consumer is a requirement under all three new state privacy laws. Privacy policies are ubiquitous in today's world both on and offline. However, as privacy laws evolve, so do the requirements in relation to privacy policies. Drafting, updating, and implementing these policies—both internally and externally—are a crucial first step in complying with privacy laws.
- ☐ **Implementing safeguards & security measures:** Cybersecurity standards and general security safeguards have evolved along with privacy laws, at an exponential rate. While the laws generally do not require specific measures, they do require that business's implement "appropriate and proportional" technical, organizational, and physical security measures.
- ☐ **New individual rights:** The laws implement new individual rights that allow individuals to request certain things of the business, such as correction of inaccurate personal information. Businesses will need to implement and maintain robust policies and procedures that allow for such requests and reasonably comply with such requests as required under the law.
- ☐ **Opt-outs:** All three new state privacy laws implement some form of individual opt out rights, along with the traditional individual privacy rights listed about. Those opt out rights allow individuals to opt out of (i) the selling or sharing of personal information; (ii) the broad use and disclosure of sensitive personal information; (iii) certain types of targeted advertising; and (iv) the processing of personal information in furtherance of decision-making that leads to legal (or similar) consequences. Understanding the response requirements and how a business is required to process such requests will be crucial as the public gains an understanding of their new rights.
- ☐ **Opt-in:** Both the Colorado and Virginia laws prohibit the processing or use of Sensitive Data without first obtaining an individual's consent. Business's that process or use location information, financial information, or other categories of Sensitive Data will need to thoroughly review their consent procedures and implement internal policies to ensure compliance.
- ☐ **Data Mapping:** The laws does not require that formal data mapping and accompanying documentation be done. However, for a business to fully comply with the laws, they must have a full and accurate understanding of (i) what information they are collecting, (ii) where the information is kept, (iii) how long the information is retained, and (iv) how the information is use or processed. Formal or informal data mapping is necessary to comply with risk assessments, data minimization requirements, and other parts of the new laws.
- ☐ **Data Minimization and Retention:** Businesses will need to review their data retention policies and procedures to ensure they comply with new laws' data minimization requirements. They must implement policies and procedures that ensure an individual's personal information is only kept as long as reasonably necessary to complete the disclosed processing activities.
- ☐ **Risk Assessments & Audits:** Formal Risk Assessments must be conducted if a business's processing of personal information presents a significant risk to consumer privacy or security in Colorado and Virginia. In California, annual cybersecurity audits will be required to determine the risk a business's activity poses to an individual's personal information. Whether a business is required to conduct and submit such assessments to state regulators will be based on fact specific inquiries depending on the nature of the information collected, the nature of the processing, and a general weighing of the benefits and risks to the individual involved.
- ☐ **Vendor Management and Contracts:** Generally, any relationship with a third party that contemplates, or could involve, access to, or the exchange of, personal information must be governed by a specific written contract. While the laws requires certain provisions, these contractual requirements are highly fact specific and require thorough review from a privacy a security point-of-view.
- ☐ **Service Providers:** The new California law creates two new subsets of third parties; service providers and contractors. Depending how a contractual relationship is setup and maintained, a third party could be considered a service provider or contractor, which benefits a business in that some of the law's more stringent provisions will not apply.

FEDERAL REGULATION

While the federal government does not have an overarching, omnibus federal privacy law, it does have a large amount of authority to implement privacy and data protection regulations on a piece-meal basis. The Federal Trade Commission acts as a default privacy agency, implementing regulations targeted at protecting consumers from unfair or deceptive trade practices. Additionally, a number of federal agencies (including the FTC, FDIC, CFPD, OCC, etc.) have rulemaking authority to implement privacy and data protection regulation on financial institutions—which is broadly defined and applicable to any entity that provides, or is involved in, financial services—under the Gramm-Leech-Bliley Act (GLBA).

Financial Institutions

Recently, the FTC published final, updated regulations under the GLBA. The new Safeguards Rule will take affect over the course of 2022 and businesses within the Rule's scope will need to comply with all requirements by December 9, 2022. Among other things, new Safeguards Rule requires financial institutions to implement specific security measures and controls, including (i) data mapping; (ii) encryption; (iii) secure software development policies and procedures; (iv) multi-factor authentication; and (v) monitoring and logging policies and procedures. Related, a financial institution must regularly test and review the above safeguards.

Additionally, financial institutions will need to implement periodic risk assessments, designate an individual to oversee and mange the security program (i.e., a Data Protection Officer or a Chief Information Security Officer), and monitor service provider compliance with such security safeguards.

Recommendation: Financial institutions will need to review their privacy and cybersecurity policies and procedures. If they do not have the specific security measures in place, they will need to implement them. Data mapping is also required in order to better understand what else a company will need to do in order to comply with the updated rule.

Banks and Bank Service Providers

The FDIC, FRB, and OCC all implemented new breach notification standards that Bank and Bank service providers must follow. The new rule's take effect on April 1, 2022 and entities falling with the rule's scope must be fully compliant by May 1, 2022.

Importantly, the scope of what is considered a "cybersecurity incident" is broader than what other laws—including U.S. state breach notification laws—impose on entities. Traditional breach notification requirements apply to unauthorized access and disclosure of data. Here, the rule applies to potential IT system disruptions or access to the underlying IT systems.

Recommendation: Banks and Banking Service Providers must expand their cybersecurity monitoring systems to track all cybersecurity incident in order to track all disruptions to the underlying functionality of the IT systems.

Government Contractors

In 2021, the U.S. Department of Justice announced the formation of a new Cyber-Fraud Initiative, under which, they will utilize the False Claims Act in order to enforce cybersecurity contractual standards and requirements on Government Contractors. Violations of the False Claims Act lead to a maximum of three times and a minimum of two times, the amount of damages suffered by the government. Because cybersecurity incidents and data breaches can lead to significant harm, Government Contractors could be liable for large sums.

Recommendation: With the DOJ's new focus on Government Contractor cybersecurity requirements, entities should be reviewing their government contracts and agreements to ensure they are complying with, and can comply with, cybersecurity and data protection obligations.

INTERNATIONAL LAWS

China

China's new Personal Information Protection Law (PIPL) took effect on November 1, 2021. The law largely tracks with other international privacy and data protection laws, both in its broad scope and the strict privacy principles that it lays out. PIPL applies to processing of PI that occurs both inside and outside of China. A processor that operates outside of China falls under the PIPL if they process PI (1) for the purpose of providing products or services to persons in China; or (2) to analyze and evaluate the behavior of persons in China. This new law is similar to Europe's GDPR in scope and applicability.

China To-Do List

- ☐ **Drafting internal and external policies:** PIPL requires that a business provide an individual with notice prior to the collection, use, or processing of their personal information. Drafting, updating, and implementing privacy policies—both internally and externally—are a crucial first step in complying with privacy laws.
- ☐ **Appoint a Data Protection Officer:** If a business meets certain thresholds (has more than 200 employees, processes over the personal information of over 1,000,000 individuals a year or the sensitive personal information of over 100,000 a year) it must appoint a Data Protection Officer.
- ☐ **Implementing safeguards & security measures:** Cybersecurity standards and general security safeguards have evolved along with privacy laws, at an exponential rate. While the law does not require specific measures, they do require that business's implement proper technical, organizational, and physical security measures. At a minimum, the security measures must be designed to protect against unauthorized access, breach, alteration, or loss of personal information.
- ☐ **New individual rights:** The law implements new individual rights that allow individuals to request certain things of the business, such as correction of inaccurate personal information. Businesses will need to implement and maintain robust policies and procedures that allow for such requests and reasonably comply with such requests as required under the law.
- ☐ **Opt-in:** A business must obtain separate consent (other than acceptance of the general privacy policy) for: (i) the processing of sensitive personal information; (ii) the overseas transfer of personal information; (iii) marketing communications; (iv) sharing or disclosing personal information with another entity who will control the data. Business will need to ensure their policies and procedures comply, including that their disclosures provide for such information and that separate consent is obtained in such situations.
- ☐ **Data Mapping & Records of Data Processing:** Under PIPL, data processing records must be retained for at least five years. This means a business must retain for five years, records that provide for the data, scale, purpose, and basic information about the sharing, disclosure, transfer, and information of the recipient involved in any data transfer.
- ☐ **Data Minimization and Retention:** Businesses will need to review their data retention policies and procedures to ensure they comply with PIPL's data minimization requirements. They must implement policies and procedures that ensure an individual's personal information is only kept as long as reasonably necessary to complete the disclosed processing activities.
- ☐ **Risk Assessments & Audits:** PIPL requires Personal Information Impact Assessments, under which, businesses review and assess potential risks and mitigation strategies and measures to be taken in light of such risks. Businesses must understand and weigh the risks involved in their collection and processing activities.
- ☐ **Data Localization and Transfer:** Under Chinese law and new draft cross-border transfer regulations, business meeting certain thresholds must retain local copies of the information they collect and meet certain requirements (such as formal security and privacy assessments and contracts with the receiving party). Further, even if a business complies with the foregoing, they will need to determine whether they have to keep a copy of transferred personal information in china.
- ☐ **Vendor Management:** Generally, any relationship with a third party that contemplates, or could involve, access to, or the exchange of, personal information must be governed by a specific written contract. While the law requires certain types of provisions, the wording and scope of the provisions are highly fact specific.

INTERNATIONAL LAWS

South Africa

South Africa began enforcement of their Protection of Personal Information Act (POPIA) on July 1, 2021. The law is modeled closely after Europe's GDPR and requires similar data protection principles and standards. Among other things, POPIA implements new individual rights, a broad definition of personal information, and forms enforcement mechanisms through a new South Africa Information Regulator.

South Africa To-Do List

- ☐ **Drafting internal and external policies:** POPIA requires that a business provide an individual with notice prior to the collection, use, or processing of their personal information. Such notices must disclose the lawful basis by which the business is collecting and processing the personal information. POPIA provides eight different lawful bases. Drafting, updating, and implementing privacy policies—both internally and externally—are a crucial first step in complying with privacy laws.
- ☐ **Appoint a Data Protection Officer:** Business must appoint a Data Protection Officer and the Data Protection Officer must be registered with South Africa's Information Regulator.
- ☐ **Implementing safeguards & security measures:** Cybersecurity standards and general security safeguards have evolved along with privacy laws, at an exponential rate. While the law does not require specific measures, it does require that business's implement "appropriate and reasonable" technical, organizational, and physical security measures. Knowing what measures to adopt and implement depends on a fact-specific analysis of the potential risks and mitigation strategies and measures that can be employed.
- ☐ **New individual rights:** The law implements new individual rights that allow individuals to request certain things of the business, such as correction of inaccurate personal information. Businesses will need to implement and maintain robust policies and procedures that allow for such requests and reasonably comply with such requests as required under the law.
- ☐ **Opt-in:** A business must obtain separate consent (other than acceptance of the general privacy policy) for: (i) the processing of sensitive personal information; (ii) the overseas transfer of personal information; (iii) marketing communications; (iv) sharing or disclosing personal information with another entity who will control the data. Businesses will need to ensure their policies and procedures comply, including that their disclosures provide for such information and that separate consent is obtained in such situations.
- ☐ **Data Mapping & Records of Data Processing:** In order to comply with POPIA, business must fully understand how personal information flows within their business systems and architecture. In order to comply with various provisions of the law (i.e., responding to consumer requests or properly conducting risk assessments), a business must conduct data mapping.
- ☐ **Data Minimization and Retention:** Businesses will need to review their data retention policies and procedures to ensure they comply with POPIA's data minimization requirements. They must implement policies and procedures that ensure an individual's personal information is only kept as long as reasonably necessary to complete the disclosed processing activities. Further use of the information requires separate individual consent.
- ☐ **Risk Assessments & Audits:** POPIA requires Personal Information Impact Assessments, under which, businesses review and assess potential risks and mitigation strategies and measures to be taken in light of such risks. Businesses must understand and weigh the risks involved in their collection and processing activities.
- ☐ **Data Localization and Transfer:** Any transfer of personal information from South Africa to a third party in another country will require either specific consent from the individual's whose personal information is being transferred, or specific contracts governing the transfer and the third parties processing of such personal information.
- ☐ **Vendor Management:** Generally, any relationship with a third party that contemplates, or could involve, access to, or the exchange of, personal information must be governed by a specific written contract. While the law requires certain types of provisions, the wording and scope of the provisions are highly fact specific.

UPDATED SCCS

As of September 2021, businesses who fall within the scope of Europe's GDPR must be using the updated and amended Standard Contractual Clauses. Contracts that were entered into prior to September 2021 can continue to rely on the old Standard Contractual Clauses. However, such contracts entered into with the old Standard Contractual Clauses must be amended to include the new Standard Contractual Clauses by Dec. 27, 2022.

A business must utilize the Standard Contractual Clauses if they are entering into contracts that involve the transfer of European personal information.

For More Information:

Michael Stovsky
mstovsky@beneschlaw.com | 216.363.4626

Alison Evans
aevans@beneschlaw.com | 216.363.4168

Ryan T. Sulkin
rsulkin@beneschlaw.com | 312.624.6398

Kris Chandler
kchandler@beneschlaw.com | 614.223.9377

Helen Schweitz
hschweitz@beneschlaw.com | 312.624.6395

Lidia C. Mowad
lmowad@beneschlaw.com | 216.363.4443

Wendy Esposito
wesposito@beneschlaw.com | 216.363.4493

Lucas Schaetzel
lschaetzel@beneschlaw.com | 312.212.4977