July 2023

Skadden

Privacy & Cybersecurity Update

SEC Adopts Rules for Cybersecurity Risk Management, Strategy and Incident Disclosure

On July 26, 2023, the Securities and Exchange Commission adopted final rules intended to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance and incident reporting by public companies that are subject to the reporting requirements of the Securities Exchange Act of 1934 (including foreign private issuers). For more information, please read Skadden's full mailing on this topic.

EU and US Agree on New Data Privacy Framework

The European Commission (EC) and the U.S. government have established a new privacy framework that allows participating companies to transfer data from the European Economic Area (EEA) to the U.S. under the EU's General Data Protection Regulation (GDPR).

Negotiations on the long-anticipated EU-U.S. Data Privacy Framework (DPF) concluded this month, and the new framework is now in force as of July 10, 2023. The new framework is based on the previous Privacy Shield, but the U.S. has taken certain additional steps to align its intelligence-gathering practices with European data protection principles, including establishing processes to enable Europe-based individuals to raise issues regarding the treatment of their information. These processes apply not just to personal data transferred under the DPF, but also to personal data transferred under other valid data transfer mechanisms, such as the EU-approved Standard Contractual Clauses (SCCs). Below, we summarize the key elements of the framework, the next steps for organizations that want to participate and some potential areas in which the framework may be subject to challenges.

Background

The GDPR prohibits the transfer of personal data from the EEA to jurisdictions that have not been deemed by the EC to have adequate data privacy protections, unless a valid data transfer mechanism is in place, which may require certain additional steps to be taken, such as entering into SCCs. Since the EC does not view the U.S. as providing adequate levels of protection for personal data, companies seeking to export personal data from the EEA to the U.S. must ensure that they have a valid transfer mechanism, such as the DPF, in place prior to any such transfer.

Until July 16, 2020, the EU-U.S. Privacy Shield was one such valid data transfer mechanism. However, the Court of Justice of the European Union (CJEU) invalidated this mechanism in *Schrems II*, holding that the U.S. regime governing access to personal data by intelligence and security services did not provide Europe-based individuals with adequate judicial remedies if their personal data was processed unlawfully. After *Schrems II*, organizations had to rely on an alternative valid data transfer mechanism to lawfully transfer personal data to the U.S., such as the SCCs with supplemental measures.[1]

On July 10, 2023, the EC approved the DPF, which recognizes the U.S. as providing an adequate level of protection for personal data transferred from the EEA to U.S. DPF-certified organizations. The DPF allows data transfers from any public or private entity in the EEA to a U.S. DPF-certified organization, without the need for additional supplemental measures to be put in place to facilitate the transfer.

The Data Privacy Framework

Eligible Companies

Any U.S. organization subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC) or Department of Transportation (DoT) is eligible to participate in the DPF. The FTC has jurisdiction over most for-profit entities in various industries, but there are some types of companies — such as banks, insurance companies, nonprofits and telecommunications service providers — over which its jurisdiction is limited or nonexistent. Ambiguities regarding the scope of the FTC's jurisdiction (even taking into account that of the DoT) may lead to some uncertainty as to what types of companies — and which subsidiaries of companies — can participate in the DPF.

Rules and Safeguards To Limit Access to Data by US Intelligence Authorities

The U.S. executive order on "Enhancing Safeguards for United States Signals Intelligence Activities," signed by President Joe Biden in October 2022, was designed to address the concerns raised by the CJEU in *Schrems II*, and forms the basis of the DPF.

The order directs the U.S. intelligence community to update its policies and procedures to comply with certain safeguards designed to protect the rights of individuals. In particular, the order states that signals intelligence activities should only be conducted to the extent they are necessary and proportionate to advance a "validated intelligence priority," the definition of which is broad. Accordingly, it remains unclear how the concept will be applied in practice.

The order also outlines other data protection safeguards, including these requirements:

- Personal data collected about Europe-based individuals by the U.S. intelligence services should be minimized.
- Any sharing of collected data should take due account of the potential for harmful impact to the individual.
- Data collected shall be subject to appropriate access and security protections.
- The nature, type and context of data collection shall be documented.

These requirements mirror core principles of the GDPR.

Redress Mechanism for Europe-Based Individuals

Under the DPF, the U.S. has implemented a two-tier redress mechanism for Europe-based individuals who wish to raise a complaint that their personal data has been processed unlawfully by U.S. authorities. Such individuals can submit a complaint to their national data protection authority, who will then pass the complaint to the European Data Protection Board (EDPB). The EDPB will transmit the complaint to U.S. authorities on the complainant's behalf. National data protection authorities will then be required keep the complainant informed of the status of their complaint. The EDPB has confirmed that Europe-based individuals do not need to demonstrate that their data was collected by U.S. intelligence agencies for a complaint to be admissible.

Complaints will be investigated in the first instance by the U.S. Director of National Intelligence's Office of Civil Liberties, Privacy and Transparency, whose civil liberties protection officer (CLPO) is responsible under the DPF for ensuring that U.S. intelligence agencies comply with the privacy and fundamental rights detailed in the order. If unsatisfied with the decision of the CLPO, Europe-based individuals can appeal a decision to the newly created Data Protection Review Court (DPRC), which is made up of six (or more) judges. The DPRC is the final appeal body in the U.S. for the DPF and the U.S. attorney general is to appoint individuals with relevant legal experience who are not currently employees of the U.S. government to serve as judges of the DPRC. The DPRC has the power to investigate complaints by obtaining relevant information from intelligence agencies and can make binding remedial decisions.

[1] See our July 17, 2020, mailing "*Schrems II*: EU-US Privacy Shield Struck Down, but European Commission Standard Contractual Clauses Survive," for our previous review of the *Schrems II* decision and the need for organizations to rely on alternative valid data transfer mechanisms.

For both complaints to the CLPO and appeals to the DPRC, the DPRC will appoint a special advocate with relevant experience who will ensure that the complainant's interests are represented in the process and that the CLPO or DPRC is properly informed of the factual and legal aspects of the case. The complainant will not be directly involved in the process.

Once the CLPO or DPRC process concludes, the complainant will be informed that either (i) no violation of U.S. law was identified or (ii) a violation was found and remedied. The complainant also will be notified when any relevant information is no longer subject to confidentiality requirements and can be obtained by the complainant. The U.S. has highlighted that its government has invested significant resources in setting up these redress mechanisms, which suggests that the processes are likely to be effective.

Self-Certification

U.S. organizations that wish to participate in the DPF should visit the official website to begin the self-certification process.[2] The process requires organizations to comply with standard data protection principles similar to those required under the EU-U.S. Privacy Shield. These requirements are:

- Informing individuals about data processing.
- Providing free and accessible dispute resolution.
- Cooperating with the U.S. government.
- Maintaining data integrity and purpose limitation.
- Ensuring accountability for data transferred to third parties.
- Ensuring commitments are kept as long as data is held.

Organizations that become DPF-certified will be required to recertify annually that they are still in compliance with the requirements of the DPF. Organizations that still participate in the EU-U.S. Privacy Shield should find the process for certification under the DPF to be relatively straightforward, given that many of the requirements of the DPF are similar.

The functioning of the DPF will be subject to periodic reviews carried out by the EC and competent U.S. authorities. The first review by the EC will take place within a year of the DPF being in force, with the period of time until the next review being decided during that first review.

Legal Challenges Likely

The DPF is likely to be subject to judicial challenge(s). Max Schrems (the complainant in *Schrems II*) has confirmed that he intends to bring a claim to the CJEU, including on the basis that the U.S. definitions of "necessary" and "proportionate" are unlikely to be aligned with the meanings given to those terms under EU law. There also are concerns surrounding whether the appointed special advocate in the redress procedures is truly independent from the process such that the complainant's case is independently presented. In addition, Europe-based individuals who seek redress will not be able to access the reasoned decisions granted by the courts unless they are declassified, with the courts having no ability to determine this classification. A restriction of the rights relating to access to an oral hearing and a reasoned judgment can, under EU law, only be restricted in the interests of national security in a limited and proportionate way. Accordingly, this may be a focus in any judicial challenge of the DPF.

At this stage, organizations may choose not to abandon other valid data transfer mechanisms in favor of the DPF just yet, given the uncertainty of any future judicial challenge(s). However, it is important to note that the measures that the U.S. government has put in place, including the redress mechanisms, apply to data transfers to the U.S. made under *any* valid transfer mechanism, even if the receiving company does not self-certify to the DPF. Thus, these measures also can act as additional safeguards in the context of other data transfer mechanisms, such as the SCCs or binding corporate rules.

The DPF also will be relevant when companies undertake data protection impact assessments, which the GDPR requires when an organization processes personal data in a manner that is "likely to result in a high risk to the rights and freedoms of natural persons." This requirement applies regardless of which data transfer mechanism a company uses in connection with an international transfer of such personal data. Even if the receiving company does not intend to self-certify to the DPF, the transferring company may take the DPF's safeguards into account when conducting this assessment.

UK Extension

A U.K. extension to the DPF, known as the U.K.-U.S. data bridge, is under negotiation between the governments of the U.S. and U.K. The U.S. Department of Commerce has issued an advisory notice confirming that U.S. organizations that self-certify for the DPF also can self-certify for the data bridge, but cannot rely on the mechanism for personal data transfers from the U.K. until the data bridge has come into force, which is expected to be sometime later in 2023.

Key Takeaways

The question of how to lawfully transfer personal data from the EEA to the U.S. has been troublesome since the introduction

[2] The website is located at www.dataprivacyframework.gov.

of the GDPR, with the DPF reflecting the most recent attempt to address the issue following the Safe Harbor (invalidated in 2016) and the aforementioned EU-U.S. Privacy Shield (invalidated in 2020). Whether the DPF will survive likely legal challenges remains to be seen, but, for now, it can be an important mechanism that companies may rely upon to assist in the smooth transfer of personal data between these two important economic regions.

Return to Table of Contents

Oregon and Texas Enact Consumer Privacy Laws

Oregon and Texas have joined the growing number of states to pass statewide consumer privacy laws in 2023.

On June 20, 2023, and July 18, 2023, respectively, Texas and Oregon joined the rapidly growing number of states that have enacted state-level consumer privacy laws. The Texas Data Privacy and Security Act (TDPSA) and the Oregon Consumer Privacy Act[3] (OCPA), are two comprehensive laws that aim to protect the personal data of consumers and are modeled on similar laws passed in states such as Virginia, Colorado and Florida, but feature some important differences.

Oregon Consumer Privacy Act

Scope of Coverage

Similar to other state privacy laws, the OCPA applies to entities (whether natural persons or organizations) that conduct business in Oregon or that otherwise provide products or services that are targeted to residents of the state that, during a calendar year, controlled or processed: (i) the personal data of not less than 100,000 consumers in Oregon, excluding personal data controlled or processed solely for the purpose of completing a payment transaction, or (ii) the personal data of not less than 25,000 consumers in Oregon if more than 25% of the entity's annual gross revenue came from selling personal data.

As in many other state privacy laws, the OCPA defines data subjects as "consumers," natural persons who are residents of the state "acting in any capacity other than engaging in commercial activity or performing duties as an employer or employee." Although "engaging in commercial activity" is potentially subject to a broad interpretation that would include customers of a business, it appears to be targeted toward information gathered in a business-to-business transaction context.

Exemptions

As with other state laws, the OCPA includes certain exemptions to the law's obligations, though they are narrower than those in some other states' laws. For example, while the OCPA excludes information that is processed in accordance with, or created to comply with, the Health Information Portability and Accountability Act (HIPAA), it does not generally exempt entities that are regulated under this federal law. Similarly, the OCPA excludes information processed in accordance with, or created to comply with, the Gramm Leach Bliley Act (GLBA), but does not generally exempt entities regulated under that law.

Additionally, as with Colorado's privacy law, the OCPA does not contain a broad exemption for nonprofits, though some specific types are exempted. However, the OCPA will not apply to nonprofits until July 1, 2025.

The OCPA broadly exempts certain types of businesses from its coverage, such as governmental bodies, financial institutions (as defined by the Bank Holding Company Act) and certain businesses in the insurance industry.

The OCPA also does not apply to activities governed by the Fair Credit Reporting Act (FCRA), specified employee-related information (such as information processed and maintained solely in connection with an individual's employment or application for employment), some non-commercial activities of certain types of organizations (such as nonprofits that provide television or radio programming in Oregon) and information that is regulated under the Airline Deregulation Act, the Driver's Privacy Protection Act, the Family Educational Rights, the Privacy Act and the Farm Credit Act in Delaware.

Key Terms and Concepts

Personal Data

Under the OCPA, the term "personal data" is defined as information "that is linked to or is reasonably linkable to a consumer or to a device that identifies, is linked to or is reasonably linkable to one or more consumers in a household." Similar to many other states' laws, "personal data" excludes deidentified data and data that has been made lawfully available to the general public or that a controller reasonably believes has been made lawfully available to the general public.

Sensitive Data

The OCPA defines "sensitive data" as personal data that reveals the below information about consumers:

- Racial or ethnic background.
- National origin.

[3] A copy of the OCPA can be found here.

- Religious beliefs.
- Mental or physical condition or diagnosis.
- Sexual orientation, status as transgender or nonbinary.
- Status as a victim of crime.
- Citizenship or immigration status.

"Sensitive data" also includes any personal data of a child, any biometric data and a consumer's past or present location data.

Controllers and Processors

Under the OCPA, a "controller" is someone who, alone or jointly, "determines the purposes and means for processing personal data," while a "processor" is a person who "processes personal data on behalf of a controller."

Consumer Rights

The OCPA provides Oregon consumers with a series of rights that largely mirror those in other state privacy laws. These rights include:

- **Right to access:** A right to confirm whether the controller is processing or has processed the consumer's personal data, and a right to know which third parties the data has been disclosed.
- **Right to data portability:** A right to request a copy of their personal data, which controllers are then required to provide in a portable and readily usable format.
- **Right to correct:** A right to require a controller to correct inaccuracies in their personal data, taking into account the nature of the data and the purpose for processing the data.
- **Right to delete:** A right to require a controller to delete their personal data.
- **Right to opt-out:** A right to opt-out from a controller's processing of their personal data if the controller is using the data for targeted advertising, for a sale or for profiling in furtherance of decisions that produce legal effects or effects of similar significance.

Consumers may exercise these rights by submitting a request to a controller using the method specified in the controller's privacy notice. Similar to most state privacy laws, the OCPA requires controllers to respond to a request within 45 days, and may, under certain circumstances, delay its response by an additional 45 days, so long as the controller notifies the consumer and explains the reason for the extension.

Obligations of Controllers

Under the OCPA, controllers are subject to certain obligations that are similar to those in many other state privacy laws.

Privacy Notice

The controller must provide a reasonably accessible, clear and meaningful privacy notice to consumers. The privacy notice requirements are more extensive than similar requirements in other states' privacy laws. Under the OCPA, the privacy notice must include this information:

- The categories of personal and sensitive data that the controller processes.
- The purpose for processing the data.
- An explanation for how a consumer may exercise their rights under the statute.
- The categories of personal and sensitive data that is shared with third parties.
- The categories of such third parties with whom the data is shared.
- A mechanism to contact the controller.
- The identity of the controller, which includes the business name that the controller is registered under in the state.
- A clear and conspicuous description of how the controller processes personal data for targeted advertising or profiling in furtherance of decisions with legal or similar significance, and how the consumer can opt out of this processing.
- The methods the controller established for a consumer to submit a personal data request.

Data Minimization

Under the OCPA, the controller must limit the collection of personal data to data that is "adequate, relevant, and reasonably necessary" to serve the purposes described in the privacy notice. If the controller is processing personal data outside of these purposes, the controller must obtain the consumer's consent.

Data Security

The controller must establish, implement and maintain safeguards that protect the confidentiality, integrity and accessibility of the personal data that it collects, uses or retains.

Revocations and Appeals

Under the OCPA, controllers must provide a means for consumers to revoke their consent to processing that is at least as easy as the means used by the consumer to provide their consent. Once the consumer revokes their consent, the controller must cease processing their personal data within 15 days.

Controllers also must establish a process under which a consumer can appeal the controller's decision to refuse a consumer's request to exercise any of their rights.

Children's Data

The OCPA includes heightened protections for children's data. The law requires that controllers receive consent prior to processing data about children aged 13-15 for the purposes of providing targeted advertising, selling the data or using the data to profile the consumer in furtherance of decisions that produce legal or similarly significant effects. Additionally, when processing a child's personal data, the controller must do so in accordance with the requirements set forth in the Children's Online Privacy Protection Act (COPPA).

Sensitive Data

Controllers must obtain consent before processing a consumer's sensitive data.

Data Protection Assessment

Controllers must conduct and document a data protection assessment on the processing of personal data for processing activities that pose a heightened risk of harm to the consumer. Such activities are listed here:

- Processing data for targeted advertising.
- Selling personal data.
- Processing sensitive data.
- Processing data for the purpose of profiling if the profiling presents a reasonably foreseeable risk of harms specified in the statute.

This requirement only applies to processing activities that occur on and after July 1, 2024, which is when the OCPA goes into effect.

Opt-Out Signals

The OCPA also requires controllers to implement opt-out preference signals. This opt-out requirement is similar to what is required under privacy laws in Montana, Colorado, Connecticut and California, but includes some key differences. The OCPA, for example, requires that a consumer must be required to affirmatively select the opt-out option, as opposed to having the opt-out option as a default setting. This obligation does not apply until January 1, 2026.

Processor Obligations

The OCPA also imposes several obligations on processors. For instance, processors must enter into a contract with the controller that has instructions for processing data, the nature and purpose of the processing, the type of data that is subject to processing and the duration of the processing. The contract also must include certain specific obligations, such as:

- Ensuring that each person that processes personal data is subject to a duty of confidentiality with respect to the personal data.
- Requiring the processor to delete the personal data or return the data to the controller at the controller's direction or at the end of the provision of services, unless a law requires the processor to retain the personal data.
- Requiring the processor to make available to the controller, at the controller's request, all information the controller needs to verify that the processor has complied with all obligations required of the processor under the act.
- Allowing the controller or its designee to assess the processor's policies and technical and organizational measures for complying with the processor's obligations.

These obligations are not as extensive as those required under California's privacy law, but are similar to those of most other states that have enacted privacy laws.

Enforcement and Effective Date

As with most other state privacy laws, there is no private right of action under the OCPA. Instead, Oregon's attorney general has exclusive authority to enforce the provisions of the act.

Prior to initiating an enforcement proceeding, the attorney general must notify the controller of its violation and allow for a cure of the violation within 60 days. If the controller fails to cure the violation, the attorney general or Oregon Department of Justice may bring an enforcement proceeding.

The OCPA is scheduled to take effect on July 1, 2024, though, as noted previously, it does not apply to nonprofits until July 1, 2025, and the opt-out signals obligations do not come into effect until January 1, 2026.

Texas Data Privacy and Security Act

Scope of Coverage

The TDPSA[4] takes a broader approach to applicability than many other states, as the law has no revenue or data-processing volume threshold for determining whether an organization is subject to the law. Instead — though the act has a number of key exceptions — the TDPSA is applicable to any business that (i) conducts business in Texas or produces products or services by Texas residents and (ii) processes or engages in the sale of personal data.

[4] The details of the TDPSA can be accessed here.

The TDPSA defines "sale" as the disclosure of personal data to a third party for "monetary or other valuable considerations."

Although, as noted, there is no revenue or volume threshold for application of the TDPSA, the act exempts "small businesses," as defined by the U.S. Small Business Administration (SBA), from most of its obligations. This exclusion may give rise to some uncertainty, however, as the SBA has multiple definitions of a "small business" based on different industries.

As in many other state privacy laws, the TDPSA defines data subjects as "consumers," which are natural persons who are residents of the state acting in any capacity "other than acting in a commercial employment context." As with the OCPA, "acting in a commercial context" is potentially subject to a broad interpretation that would include customers of a business, though the language appears to be targeted toward information gathered in the context of a business-to-business transaction.

Entity Exemptions

The TDPSA also includes exemptions that are similar to those in various other states laws, such as for nonprofits, institutions of higher education, financial institutions governed by the GLBA and entities governed by HIPAA (including not just HIPAA's "covered entities," but also their business associates). Note that with respect to the GLBA and HIPAA exclusions, the TDPSA differs from the laws in states such as Oregon and Delaware, which only exclude the information subject to those laws rather than the entire entity.

Data Exemptions

In addition to the entity-level exemptions, the TDPSA also exempts certain types of data, such as (i) data processed in the employment context, (ii) protected health information under HIPAA and other health records, and (iii) data subject to certain other law such as the FCRA, the Driver's Privacy Protection Act, the Farm Credit Act and the Family Educational Rights and Privacy Act.

Key Terms and Concepts

Personal Data

Under the TDPSA, "personal data" is "any information, including sensitive data, that is linked or reasonably linkable to an identified or identifiable individual."

The act also expressly includes pseudonymous data "when the data is used by a controller or processor in conjunction with additional information that reasonably links the data to an identified or identifiable individual." On the other hand, as in many other state privacy laws, the TDPSA excludes "deidentified data or publicly available information" from "personal data." Therefore, data that does not identify an individual is not subject to the TDPSA unless it is used in conjunction with other data that does identify said individual.

Sensitive Data

Similar to other recent state privacy laws, the TDPSA includes specific obligations with respect to "sensitive data." Specifically, "sensitive data" is personal data that reveals a consumer's:

- Racial or ethnic origin.
- Religious beliefs.
- Mental or physical health diagnosis.
- Sexuality.
- Citizenship or immigration status.

"Sensitive data" also includes genetic or biometric data processed to identify individuals, personal data collected from a known child or precise geolocation data (*i.e.*, identifies a consumer within a radius of 1,750 feet).

Key differences between the TDPSA and other states' laws regarding the scope and definition of "sensitive data" include the use of the term "sexuality" Instead of such phrases as "sexual orientation," which are used in the privacy laws in Montana and Florida, for example. Another difference is that the TDPSA limits its protection of health information to that which is specifically related to a "mental or physical diagnosis," as opposed to additional categories of health information used in other states' laws.

Controllers and Processors

Under the law, a "controller" of personal data is the person that determines the purpose and means of processing personal data, while the "processor" is the person who processes the personal data on the controller's behalf.

Consumer Rights

The TDPSA provides consumers with a series of specific rights with respect to their personal data, which are similar to those in other states' laws. Specifically, consumers have the following rights under the TDPSA:

- **Right to access:** A right to confirm whether the controller is processing or has processed the consumer's personal data.
- **Right to data portability:** A right to request a copy of their personal data, which controllers are then required to provide in a portable and readily usable format.

- **Right to correct:** A right to require a controller to correct inaccuracies in their personal data, taking into account the nature of the data and the purpose for processing the data.
- **Right to delete:** A right to require a controller to delete their personal data.
- **Right to opt-out:** Consumers have the right to opt-out from a controller's processing of their personal data if the controller is using the data for targeted advertising, for the sale of the data or for profiling in furtherance of decisions that produce legal effects or effects of similar significance.

Consumers may exercise these rights by submitting a request to a controller using the method specified in the controller's privacy notice. Similar to most state privacy laws, the controller must respond to a request within 45 days and may, under certain circumstances, delay its response by an additional 45 days, so long as the controller notifies the consumer and explains the reason for the extension.

Obligations of Controllers

Under the TDPSA, controllers are subject to certain obligations that are similar to those in many other state privacy laws.

Privacy Notice

The controller must provide a reasonably accessible, clear and meaningful privacy notice to consumers. The privacy notice requirements are more extensive than similar requirements in other states' privacy laws. The privacy notice must include descriptions of:

- The categories of personal and sensitive data that the controller processes.
- The purpose for processing the data.
- An explanation for how a consumer may exercise their rights under the statute.
- The categories of personal data that are shared with third parties.
- The categories of such third parties with whom the data is shared.
- A method to contact the controller.

In addition, if a controller sells sensitive or biometric personal data, it must post a specific notice in its privacy notice, saying one of the two following statements, as applicable:

- NOTICE: We may sell your sensitive personal data.
- NOTICE: We may sell your biometric personal data.

Data Minimization

The controller must limit the collection of personal data to that which is "adequate, relevant, and reasonably necessary" to serve the purposes described in the privacy notice. If the controller is processing personal data outside of these purposes, the controller must obtain the consumer's consent.

Data Security

The controller must establish, implement and maintain safeguards that protect the confidentiality, integrity and accessibility of the personal data that it collects, uses or retains.

Revocations and Appeals

Unlike some other state laws, the TDPSA does not require controllers to provide a means by which consumers can revoke their consent to processing. However, controllers must establish a process under which a consumer can appeal the controller's decision to refuse a consumer's request to exercise any of its rights.

Children's Data

When processing a child's personal data, the TDPSA requires controllers to do so in accordance with the requirements set forth in COPPA.

Sensitive Data

Controllers must obtain consent before processing a consumer's sensitive data. This is true even for small businesses, which are otherwise not subject to TDPSA's requirements.

Data Protection Assessment

The TDPSA requires controllers to conduct the assessments of processing activities that involve these actions:

- The processing of data for purposes of targeted advertising.
- The sale of personal data.
- The processing of data for purposes of profiling if certain risk factors are met.
- The processing of sensitive data.
- Any processing activities that present a heightened risk of harm to consumers.

These assessments will be made available to the Texas attorney general on a confidential basis.

Opt-Out Signals

The TDPSA also requires controllers to implement opt-out preference signals. This opt-out requirement is similar to what is

required under the Montana, Colorado, Connecticut and California laws, though the version in Texas' law is not as broadly applicable. For instance, the TDPSA requires that a consumer must be required to affirmatively select the opt-out option, as opposed to a default setting. This obligation does not apply until January 1, 2025.

Processor Obligations

Similar to other states' laws, the TDPSA imposes some obligations on processors. For example, processors must enter into a contract with the controller that has instructions for processing data, the nature and purpose of the processing, the type of data that is subject to processing and the duration of the processing. It also must include certain specific obligations, such as:

- Ensuring that each person who processes personal data is subject to a duty of confidentiality with respect to the personal data.
- Requiring the processor to delete the personal data or return the personal data to the controller at the controller's direction or at the end of the provision of services, unless a law requires the processor to retain the personal data.
- Requiring the processor to make available to the controller, at the controller's request, all information the controller needs to verify that the processor has complied with all obligations the processor has under the act.
- Allowing the controller or its designee to assess the processor's policies and technical and organizational measures for complying with the processor's obligations.

These obligations are not as extensive as those required under California's privacy law, but are similar to those of most other states' privacy laws.

Dark Patterns

Unlike the OCPA, the TDPSA also attempts to tackle the issue of "dark patterns," which the act defines as "a user interface designed or manipulated with the effect of substantially subverting or impairing user autonomy, decision-making, or choice, and includes any practice the Federal Trade Commission refers to as a dark pattern."

Simply put, a dark pattern is a manipulative and mandatory design choice that forces website users to perform actions that suit the interests of the website or business. Examples may include "hidden costs," which is a cost that is shown initially but that increases as the buyer moves ahead with a payment, or "forced continuity," which is when a website requires information or card details for the user to move ahead with using the website, product or service.

The prohibition of dark patterns appears in some other states' digital privacy laws, including California.

Enforcement and Effective Date

As with most other state privacy laws, there is no private right of action under the TDPSA. Instead, the state's attorney general has exclusive enforcement power and can impose civil penalties up to $7,500 per violation. Additionally, the attorney general may recover reasonable attorneys' fees and other reasonable expenses incurred in investigating and bringing an action under the TDPSA.

Prior to initiating an enforcement proceeding, the attorney general must notify the controller of its violation and allow the controller to cure the violation within 30 days. If the controller fails to cure the violation, the attorney general may bring an enforcement proceeding.

The TDPSA will take effect on March 1, 2024, with the opt-out signals obligations set to take effect in January 1, 2025.

Key Takeaways

- States have been passing privacy laws at an accelerating pace, and more are on the way (Delaware, for example, has passed a law, but as of this writing it has not yet been signed by the state's governor). With state legislatures becoming more concerned about the use of consumer data, companies should stay vigilant to ensure that they are in compliance with these laws and be aware of similar laws in the process of being passed in other states.
- With the exception of California's privacy law, the recently enacted state laws have largely followed the same model, though each piece of legislation has unique adjustments to certain aspects of data protection, meaning companies would be advised to pay close attention to each law passed.
- It seems unlikely that these variations in the laws will conflict with each other, which will likely lead many companies to adopt a "highest common denominator" approach to privacy practices in the U.S. through the adoption of a single approach that meets all of the multiple state requirements.

Return to Table of Contents

California Court Delays Enforcement of CPRA Regulations

A California court has delayed the enforcement of new regulations under the California Consumer Privacy Act of 2018 (CCPA) that implemented changes required by the California Privacy Rights Act (CPRA).

On June 30, 2023, shortly before their enforcement date of July 1, 2023, a Sacramento County Superior Court judge stayed the enforcement of CPRA regulations, delaying the compliance deadline for businesses subject to the law. The court agreed with the California Chamber of Commerce that the plain language of the CPRA contemplated that enforcement should not take effect until one year from the date that regulations were finalized by the California Privacy Protection Agency (CPPA). For the majority of the covered issues, regulations will take effect on March 29, 2024. The remaining areas will have an enforcement date that is one year from the release of the finalized regulations.

Background

In 2018, the California State Legislature enacted the CCPA, giving consumers more control over their personal information and restricting the ways that businesses can collect such information. In 2020, California voters approved the CPRA, which added additional privacy safeguards for consumers and took effect on January 1, 2023. The CPRA created the CPPA to implement and enforce the new privacy legislation. The CPRA established two key deadlines: July 1, 2022, for the CPPA to promulgate final regulations to implement the CPRA, and July 1, 2023, as the enforcement date for those regulations. Pursuant to the California Administrative Procedure Act, the CPPA commenced efforts to promulgate regulations under the CPRA.

In February 2022, the CPPA conceded that it would not be able to comply with the initial July 1, 2022, deadline to promulgate the final regulations. As of March 29, 2023, the CPPA had finalized regulations on only 12 of the 15 mandatory issues contemplated by the CPRA. The final three areas — cybersecurity audits, risk assessments and automated decision-making technology — would not have finalized regulations until after the July 1, 2023, statutory enforcement date.

In light of the delayed finalization of the regulations, the California Chamber of Commerce filed an action to delay the July 1, 2023, enforcement date, arguing that businesses would be unfairly prejudiced if the CPPA began enforcing its regulations on that date.

Court Postpones Enforcement

On June 30, 2023, a Sacramento County Superior Court judge agreed to delay the enforcement of the new CCPA until March 29, 2024. Relying on the plain language of the statute, the court agreed that the CPPA had a mandatory duty to adopt final regulations by July 1, 2022. In the absence of finalized regulations by the deadline, the court held that California voters' intent was to have a 12-month window between the passing of final regulations in an individual area and the CPPA's enforcement. While the Chamber of Commerce argued that there should be a blanket ban on enforcement until one year after *all* regulations had been finalized, the court agreed that the voters' intent would be thwarted by "delaying the Agency's ability to enforce any violation of the Act for 12 months after the last regulation" was finalized.

In its final disposition, the Sacramento County Superior Court stayed the enforcement of the new CCPA regulations until a period of "12 months from the date that [the] individual regulation becomes final." For those areas where regulations had been finalized in March 2023, the new enforcement date was pushed to March 29, 2024. For the three areas where the CPPA has not yet finalized its regulations, the enforcement will be delayed one year from the date that the agency announces finalized regulations.

Key Takeaways

While businesses covered under CCPA need not immediately comply with the regulations promulgated under the CPRA, the delay is only temporary. Businesses should be prepared to finalize their compliance with the new regulations as the majority of the regulations are set to take effect in the coming year.

Return to Table of Contents

NYDFS Updates Proposed Amendments to Cybersecurity Regulations

The New York Department of Financial Services (NYDFS) has announced a proposed set of amendments to its regulations on cybersecurity for financial services companies.

On June 28, 2023, the NYDFS announced a set of proposed amendments to its regulations setting out certain cybersecurity requirements. The amendments cover a wide range of topics, including management-level responsibility for cybersecurity issues, the role of risk assessments and response plans in the event of cybersecurity events, and notification and compliance procedures regarding the NYDFS. Many covered entities will

have to undergo a substantial overhaul of their current cybersecurity policies in order to ensure compliance with the proposed regulations.

Background

On March 1, 2017, the NYDFS promulgated regulations establishing certain cybersecurity requirements for financial services companies. In 2022, the NYDFS proposed an amendment to the cybersecurity regulations that provided for additional compliance requirements for "covered entities." The newly revised draft released in June 2023 will undergo an additional 45-day comment period before it is finalized.

The 2023 proposed amendment includes a number of notable revisions, discussed below.

Summary of Key Changes

Definition of 'Class A Companies'

Under the existing NYDFS cybersecurity regulations, a "covered entity" includes any person operating under a "license registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law, or the Financial Services Law." Underneath the umbrella of covered entities, certain additional requirements are imposed on "Class A companies," which are defined as covered entities with at least $20 million in gross annual revenue in the last two fiscal years from business operations of the covered entity and its affiliates in New York and one of these two parameters:

- Over 2,000 employees averaged over the period, including both employees of the covered entity and its affiliates.
- Over $1 billion in gross annual revenue in the period from all business operations of the covered entity and its affiliates.

The amendment clarifies that for purposes of Class A companies, when calculating the number of employees and gross annual revenue mentioned above, affiliates include only those entities that share information systems, cybersecurity resources or all or part of a cybersecurity program with the covered entity.

Audits of Cybersecurity Program

The proposed amendments clarify the types of audits that Class A companies must conduct of their cybersecurity programs. Under the existing regulations, each covered entity is required to maintain a cybersecurity program designed to protect the confidentiality and integrity of its information systems and Class A companies must audit these programs at least annually. The proposed amendment clarifies that an audit conducted by *either* internal or external auditors will qualify, so long as those conducting the audit are free to make decisions without being influenced by the covered entity or its managers.

Governance Responsibilities: Senior Governing Bodies and CISOs

Under the existing regulations, each covered entity must maintain a written cybersecurity policy, approved annually by a "senior governing body." The proposed amendment clarifies that the senior governing body may be the board of directors (or an appropriate committee) or an equivalent governing body. Additionally, the senior governing body must include all of these elements:

- Exercise effective oversight over the entity's cybersecurity risk management.
- Have sufficient understanding of cybersecurity related matters to exercise such oversight.
- Ensure that the entity's executive management implements and maintains the cybersecurity program.

The proposed amendments would require each covered entity to designate a chief information security officer (CISO), who would have a number of specific obligations. Among other duties, the CISO must provide a written report at least annually to the senior governing body regarding the entity's cybersecurity program, as well as an update to the senior governing body on any material cybersecurity issues.

Risk Assessment

Under the proposed amendment, each covered entity would be required to adopt a program of vulnerability management that assesses the effectiveness of the cybersecurity program. As part of the risk assessment, the covered entity must:

- Perform penetration testing of the entity's information systems from both inside and outside the system, conducted by a qualified internal or external party, at least annually.
- Conduct automated scans of information systems, with a manual review of any systems not covered by the automated scan, to analyze any vulnerabilities that may exist.

Based on the risk assessment, each covered entity must limit user access privileges to those necessary for an individual user to conduct her or her job, and limit the number of privileged accounts given to required users. At least annually, the covered entity must review all user access privileges and remove or disable accounts that are no longer necessary.

Authentication Requirements

The proposed amendment would clarify that covered entities must use multi-factor authentication or any individual accessing

any of the covered entity's information systems, including for remote access to its own information systems, remote access to third party applications, and all privileged accounts. The CISO may approve a more secure method of accessing the systems, but the control method must be reviewed at least annually.

Cybersecurity Event Response Plans: Incident Response and Business Continuity

The proposed amendment would require each covered entity to establish a written incident response plan designed to respond to and recover from any cybersecurity event that materially affects the confidentiality or integrity of the entity's information systems. The plan must address certain key issues, including internal processes, decision-making authority, detection, documentation, and post-event evaluation, analysis and response.

The proposed amendment also would require covered entities to implement a business continuity and disaster recovery plan. The plan must ensure these elements are met:

- Ensure the availability and functionality of information systems and services to protect the entity's personnel, assets and confidential information following a cybersecurity-related disruption to normal business activities.
- Identify any documents, systems or personnel essential to the continued operation of the business.
- Identify decision-making authority.
- Include procedures for maintenance of backup information and facilities.

Along with the requirement to maintain a business continuity plan, each covered entity must test its incident response and plan at least once annually, as well as the entity's ability to restore critical data and information systems from backups.

Notification of Cybersecurity Events

The proposed amendment would clarify the regulations' existing cybersecurity incident reporting requirements. Specifically, the proposal would make clear that the reporting requirement applies not only to events that directly affected the covered entity, but also to those that affect its noncovered entity affiliates or services providers, if any of the following applies:

- Notice of the event is required to any government body, self-regulatory agency or other supervisory body.
- The event has a reasonable likelihood of materially harming normal business operations.
- The event is one in which an unauthorized user has gained access to a privileged account.
- The event is one in which ransomware has been deployed within a material part of the covered entity's information system.

Covered entities must promptly provide any information requested and will have a continuing obligation to update and supplement the information provided.

Certification of Compliance

The proposed amendment would revise the self-certification process for covered entities. Specifically, it would soften the self-certification to material compliance with the regulations, and would add that the certification must be based on data and documentation sufficient to accurately determine and demonstrate compliance. Alternatively, the amendment would allow the entity to submit a written acknowledgement that it did not fully comply will all aspects of the regulations as required, accompanied by a remediation timeline.

The certification or acknowledgement must be signed by the entity's highest-ranking executive and its CISO. Furthermore, each covered entity must maintain all records and data supporting the certification or acknowledgement for a period of five years, to be available for examination and inspection by the NYDFS.

Extortion Payments

Finally, the proposed amendment would add an obligation for covered entities to report extortion payments made in connection with cybersecurity incidents. An initial notice of the payment would have to be made within 24 hours of the payment, and a follow up notice describing the circumstances and need for the payment — including the diligence performed to ensure compliance with applicable rules and regulations, such as those of the Office of Foreign Assets Control — would have to be made within 30 days of the payment.

Comment Period

The 45-day public comment period for the proposed amendment to the cybersecurity regulations will close on August 14, 2023.

Key Takeaways

The proposed second amendment to the NYDFS cybersecurity regulations will impose substantial requirements on financial service companies to ensure their cybersecurity programs are compliant. The regulations — including maintaining a cybersecurity program, identifying a CISO and senior governing body, and notification and compliance to NYDFS — would require covered entities to implement various company-wide policies and procedures. The regulations, while robust, ensure that finan-

cial services companies in New York are properly positioned to prepare, identify and respond to malicious cybersecurity attacks that would have a negative impact on personnel and business operations.

Return to Table of Contents

General Liability Insurer Must Defend Insured Retailer in BIPA Lawsuit

Relying in part on recent Seventh Circuit precedent, on July 5, 2023, an Illinois district court held that general liability insurer Continental Western Insurance Company (Continental) has a duty to defend its insured, Illinois grocery store chain Tony's Finer Foods Enterprises, Inc., et al. (Tony's) in a putative class action alleging that Tony's violated the Illinois Biometric Information Privacy Act (BIPA) by unlawfully collecting employees' fingerprint data.[5]

BIPA Lawsuit

In December 2018, Charlene Figueroa, a former Tony's employee, commenced a putative class action on behalf of herself and similarly situated individuals who worked for Tony's alleging that the company unlawfully collected, stored, used or disseminated employees' fingerprints in violation of BIPA. According to the complaint, as a condition of her employment, Ms. Figueroa was required to scan her fingerprints to track the hours she worked. The complaint further alleges that Tony's unlawfully stored the fingerprint data, failed to obtain a release to allow it to collect, store, use or disseminate the data, and unlawfully disclosed the fingerprint data to at least one third party and possibly others.

Tony's sought coverage for the lawsuit under its general liability insurance policy issued by Continental which, as relevant here, insured sums that Tony's became legally obligated to pay because of "personal and advertising injury," defined, in relevant part, as an "injury . . . arising out of . . . [o]ral or written publication, in any manner, of material that violates a person's right of privacy." Continental denied coverage, invoking three exclusions applicable to the "personal and advertising injury" coverage:

- "**Recording and Distribution of Material or Information in Violation of Law Exclusion (Violation of Law Exclusion)**," which bars coverage for any action or omission that actually or allegedly violates: (i) the Telephone Consumer Protection Act; (ii) the CAN-SPAM Act of 2003; (iii) the FCRA and the Fair and Accurate Credit Transactions Act; or "(iv) Any . . . statute, ordinance or regulation . . . that addresses, prohibits or limits the printing, dissemination, disposal, collecting, recording, sending, transmitting, communicating or distribution of material or information."
- "**Access or Disclosure of Confidential or Personal Information Exclusion (Access to Information Exclusion)**," which bars coverage for injury "arising out of any access to or disclosure of any person's or organization's confidential or personal information, including patents, trade secrets, processing methods, customer lists, financial information, credit card information, health information or any other type of nonpublic information."
- "**Employment-Related Practices Exclusion**," which bars coverage for injury to a person arising out of any "[e]mployment-related practices, policies, acts or omissions, such as coercion, demotion, evaluation, reassignment, discipline, defamation, harassment, humiliation, discrimination or malicious prosecution directed at that person."

In July 2022, Continental filed suit against Tony's in the U.S. District Court for the Northern District of Illinois seeking a declaration that the insurer had no duty to defend or indemnify Tony's in the BIPA lawsuit. The parties filed cross motions for judgment on the pleadings with respect to Continental's duty to defend Tony's pursuant to the policy's "personal and advertising injury" coverage. The court sided with Tony's.

The district court first found that the BIPA lawsuit triggered the policy's "personal and advertising injury" coverage, reasoning that the complaint alleges that (i) Tony's improperly disclosed its employees' fingerprint data to at least one third party in violation of BIPA and (ii) Ms. Figueroa and others similarly situated have suffered injury, including mental anguish, based on the improper disclosure of their biometric data to third parties.

The district court then turned to the exclusions, finding that none barred coverage. In concluding that the Violation of Law Exclusion was inapplicable, the district court found that the Seventh Circuit's recent opinion in *Citizens Insurance Co. of America v. Wynndalco Enterprises, LLC*[6] — which held that a materially identical policy exclusion was ambiguous and must be construed in favor of the insured — was dispositive of the issue.

The court then went on to find that the Access to Information Exclusion did not bar coverage for the BIPA lawsuit, rejecting Continental's broad reading of the exclusion by stating it "would eliminate a vast swath of privacy violation claims based on the

[5] *Continental Western Ins. Co. v. Tony's Finer Foods Enters., Inc., et al.*, No. 22-cv-3575, 2023 WL 4351469 (N.D. Ill. July 5, 2023).

[6] We reported on this decision in our June 2023 *Privacy & Cybersecurity Update*.

publication of personal information that the insuring agreement otherwise purports to cover." The court therefore concluded that the exclusion was ambiguous and — after an unsuccessful attempt to resolve the ambiguity — construed the exclusion in favor of Tony's.

Evaluating the Employment-Related Practices Exclusion, the court determined that the plain language of the exclusion "unambiguously does not encompass the *Figueroa* Lawsuit." The court reasoned that to fall within the exclusion the underlying claim must involve an action related to a specific employee's performance, and "it cannot be said that Tony's general policy of requiring fingerprint scanning to track employees' time, and its failure to secure employees' informed consent, was targeted at Figueroa or any specific employee, nor do such policies relate to any particular employee's performance." Moreover, while fingerprinting can be described as an employment practice, it is a "categorically different type of practice than everything else in the list" — defamation, harassment, humiliation, discrimination and similar behavior — and "would stick out like a sore thumb." Accordingly, the court denied Continental's motion and granted Tony's, holding that the insurer has a duty to defend Tony's in the BIPA lawsuit.

Key Takeaways

The district court decision in *Tony's Finer Foods*, as in the Seventh Circuit's recent decision in *Wynndalco*, relied in part on perceived ambiguities in the policy exclusions in determining that the insurer had a duty to defend the underlying BIPA lawsuits. These ambiguities, coupled with conflicting case law in the BIPA coverage landscape, may prompt insurers to modify their policies to clarify coverage for BIPA claims. In this vein, both insurers and policyholders must be vigilant in reviewing policy language to ensure that it aligns with the parties' understanding and expectations.

Return to Table of Contents

Privacy & Cybersecurity Update

Contacts

Stuart D. Levi
Partner / New York
212.735.2750
stuart.levi@skadden.com

James Carroll
Partner / Boston
617.573.4801
james.carroll@skadden.com

Avia M. Dunn
Partner / Washington, D.C.
202.371.7174
avia.dunn@skadden.com

Brian Duwe
Partner / Chicago
312.407.0816
brian.duwe@skadden.com

David Eisman
Partner / Los Angeles
213.687.5010
david.eisman@skadden.com

Maya P. Florence
Partner / Boston
617.573.4805
maya.florence@skadden.com

Todd E. Freed
Partner / New York
212.735.3714
todd.freed@skadden.com

Marc S. Gerber
Partner / Washington, D.C.
202.371.7233
marc.gerber@skadden.com

Richard J. Grossman
Partner / New York
212.735.2116
richard.grossman@skadden.com

Ken D. Kumayama
Partner / Palo Alto
650.470.4553
ken.kumayama@skadden.com

Michael E. Leiter
Partner / Washington, D.C.
202.371.7540
michael.leiter@skadden.com

William Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

Jason D. Russell
Partner / Los Angeles
213.687.5328
jason.russell@skadden.com

David Schwartz
Partner / New York
212.735.2473
david.schwartz@skadden.com

David Simon
Partner / Washington, D.C.
202.371.7120
david.simon@skadden.com

Ingrid Vandenborre
Partner / Brussels
32.2.639.0336
ingrid.vandenborre@skadden.com

Helena Derbyshire
Of Counsel / London
44.20.7519.7086
helena.derbyshire@skadden.com

Nicole L. Grimm
Counsel / Washington, D.C.
202.371.7834
nicole.grimm@skadden.com

Peter Luneau
Counsel / New York
212.735.2917
peter.luneau@skadden.com

James S. Talbot
Counsel / New York
212.735.4133
james.talbot@skadden.com

Eve-Christie Vermynck
Counsel / London
44.20.7519.7097
eve-christie.vermynck@skadden.com

Skadden, Arps, Slate, Meagher & Flom LLP
One Manhattan West
New York, NY 10001
212.735.3000