Skadden

Privacy & Cybersecurity Update

1 Tennessee Enacts Business-Friendly Comprehensive Consumer Privacy Law

5 Indiana Enacts Consumer Privacy Law

7 European Court of Justice Issues Three Key GDPR Rulings

8 California Privacy Protection Agency Announces Potential Regulation Proposals During May Board Meeting

9 Furniture Company Files Coverage Action Against Crime Insurer After Sustaining Wire Fraud Losses

10 Professional Liability Insurer Seeks Declaration Stating It Does Not Owe Coverage to Attorney for Claims Arising From Hacking Incidents

Tennessee Enacts Business-Friendly Comprehensive Consumer Privacy Law

When Gov. Bill Lee signed the Tennessee Information Protection Act (TIPA) into law on May 11, 2023, after its unanimous passage through the state legislature, Tennessee became the latest state to contribute to the United States' patchwork privacy landscape. While the TIPA contains several "first-of-its-kind" business-favorable provisions, including a built-in affirmative defense, it is otherwise largely based upon existing privacy laws of other states. As such, many businesses subject to comprehensive consumer privacy laws enacted in other states will be well-positioned to comply with the TIPA when it goes into effect on July 1, 2025.

Scope of the TIPA

The TIPA applies to organizations with revenue exceeding $25 million that conduct business in, and produce products or services targeted to residents of, Tennessee and that either:

- control or process personal information of at least 25,000 consumers and derive more than 50% of their gross revenue from the sale of personal information; or
- control or process the personal information of at least 175,000 consumers during a calendar year.

By comparison, Virginia's state privacy law, which the TIPA is largely based upon, does not have a revenue threshold and applies to entities that either derive over half of their gross annual revenue from the sale of personal data or control or process the personal data of 100,000 Virginia residents annually.

The term "personal information" is defined as information that is linked or reasonably linkable to an identified or identifiable natural person. However, akin to many other comprehensive state privacy laws, certain types of data and categories of entities are exempt under the TIPA. The types of personal information not subject to the TIPA include, *inter alia*, protected health information under the Health Insurance Portability and Accountability Act (HIPAA), data subject to the Gramm-Leach-Bliley Act (GLBA) and personal or educational information regulated by the Family Educational Rights and Privacy Act (FERPA).

In addition to the exclusion of the aforementioned categories of data, the TIPA also exempts governmental entities of the state of Tennessee; nonprofit organizations; financial institutions (and their affiliates) subject to the GLBA; institutions of higher education; covered entities or business associates subject to HIPAA and the Health Information Technology for Economic and Clinical Health Act; and personal information for use in a consumer report, to the extent the information is regulated by and authorized under the Fair Credit Reporting Act. Additionally — unique to the TIPA — insurance companies licensed under Tennessee law also are exempt.

As with all of the other states that have general privacy laws (other than California), the term "consumer" only applies to natural persons who are Tennessee residents acting in a personal context and not commercial or employment, such that personal information processed or maintained in the course of employment also is excluded from the scope of the TIPA.

Finally, the TIPA includes a provision expressly stating that the law does not require any person to disclose trade secrets.

Obligations of Controllers

Under the TIPA, a "controller" — defined as any natural or legal person that, alone or jointly with others, determines the purpose and means of processing personal information — has the following affirmative obligations:

- **Data minimization.** The collection of personal information by controllers must be limited to what is adequate, relevant and reasonably necessary in relation to the purposes for which the data is processed, as disclosed to the consumer.
- **Data security practices.** To protect the confidentiality, integrity and accessibility of personal information, reasonable administrative, technical and physical data security practices that are appropriate to the volume and nature of the personal information at issue must be established, implemented and maintained by controllers.
- **De-identified data.** Controllers are permitted to retain de-identified data — *i.e.*, data that cannot reasonably be linked to an identified or identifiable natural person, or a device linked to that individual — provided that they (i) take reasonable measures to ensure that such data cannot be associated with a natural person, (ii) publicly commit to maintaining and using such data without attempting to reidentify the data and (iii) contractually obligate recipients of such data to comply with the TIPA.
- **Privacy notice.** Controllers must provide consumers with a reasonably accessible, clear and meaningful privacy notice outlining (i) the categories of personal information being processed, (ii) the purpose for the processing, (iii) how consumers may exercise their consumer rights, (iv) the categories of personal information sold to third parties and (v) the categories of such third parties to whom the personal information is sold.
- **Data protection assessments.** The TIPA requires controllers to conduct and document data protection assessments of (i) processing activities involving personal information for targeted advertising, (ii) the sale of personal information, (iii) certain profiling activities and activities that present a reasonably foreseeable risk of certain types of substantial injuries to consumers, (iv) the processing of sensitive data and (v) any other processing activities involving personal information that present a heightened risk of harm to consumers. In an effort to reduce the compliance burden (taking into consideration that a similar requirement is imposed under comprehensive consumer privacy laws in California, Colorado, Connecticut, Indiana and Virginia), the TIPA permits controllers to rely upon data protection assessments conducted to comply with other laws, rules or regulations that "have a reasonably comparable scope and effect." Even though the TIPA does not go into effect until July 1, 2025, its data protection assessment requirements, while not retroactive, apply to processing activities created or generated on or after July 1, 2024, and such assessments, while confidential, must be provided to the Tennessee attorney general upon request.

Under the TIPA, the "sale of personal information" means the exchange of personal information for valuable monetary consideration by a controller to a third party, but expressly excludes (i) disclosure of personal information to a processor that processes the personal information on behalf of the controller, (ii) disclosure of personal information to a third party for purposes of providing a product or service requested by the consumer, (iii) the transfer or disclosure of personal information to an affiliate of the controller, (iv) the disclosure of information that the consumer both intentionally made available to the general public via a channel of mass media and did not restrict to a specific audience and (v) the transfer or disclosure of personal information to a third party as an asset that is part of a transaction in which the third party assumes control of all or part of the controller's assets (*e.g.*, a merger, acquisition or bankruptcy). If a controller sells personal information to third parties or processes personal information for targeted advertising, it must clearly and conspicuously disclose, and instruct consumers how to opt-out of, such sale or processing.

The TIPA defines the term "sensitive data" as a category of personal information that includes (i) personal information revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status; (ii) the processing of genetic or biometric data for the purpose of uniquely identifying a natural person; (iii) personal information collected from a known child under 13 years of age; and (iv) precise geolocation data.

In addition to the aforementioned affirmative obligations, the TIPA expressly prohibits controllers from the following:

- **Anti-discrimination.** Discrimination by controllers against consumers for exercising their consumer rights under the TIPA is prohibited.
- **Processing sensitive data.** Without the relevant consumer's consent, or parental consent in the case of a known child under the age of 13, controllers cannot process sensitive data.
- **Proportionality.** Without the relevant consumer's consent, controllers cannot process personal information for purposes that are beyond what is reasonably necessary to, and compatible with, the disclosed purposes for which the personal information is processed, as disclosed to the consumer.

Obligations of Processors

The TIPA also imposes certain obligations on processors. A "processor" is defined under the TIPA as a natural or legal entity that processes personal information on behalf of a controller. In addition to adhering to the controller's instructions, the processor must assist the controller in meeting its obligations under the TIPA. Such assistance must include (i) taking into account the nature of processing and the information available to the processor, by appropriate technical and organizational measures, to fulfill the controller's obligation to respond to consumer rights requests and (ii) providing information necessary to enable the controller to conduct and document data protection assessments.

All data processing must be conducted by a processor pursuant to a written contract between the controller and processor governing the nature, purpose and duration of the processing, as well as what personal information may be processed and the parties' respective rights and obligations. Such contract also must require the processor to (i) delete or return to the controller all personal information at the controller's discretion, (ii) ensure that all persons processing personal information are subject to a duty of confidentiality with respect to such information, (iii) demonstrate compliance with the TIPA upon the controller's reasonable request, (iv) allow and cooperate with all reasonable data assessments by or on behalf of the controller or otherwise provide the controller with its own data assessment report and (v) subject any subcontractors to the same obligations as the processor.

The foregoing requirements for controllers and processors under the TIPA are generally aligned with other state privacy laws. For instance, the TIPA's data minimization and proportionality standards are similar to those in the laws in Colorado and Connecticut; the TIPA's data protection assessment requirement is similar to that of California, Colorado, Connecticut, Indiana and Virginia; the TIPA's discrimination prohibition is similar to that of California, Connecticut, Utah and Virginia; the TIPA's consumer consent requirements to process sensitive data are similar to those in Colorado, Connecticut and Virginia; and the TIPA's contractual requirements to use third-party contractors and processors are similar to those in Indiana and Virginia. On the other hand, unlike the privacy laws of California, Colorado and Connecticut, the TIPA does not require controllers to recognize opt-out preference signals from internet web browsers.

Affirmative Defense for Businesses

In a first-of-its-kind provision among enacted state privacy laws,[1] the TIPA expressly provides that a controller or processor has an affirmative defense to a cause of action for a TIPA violation if such controller or processor creates, maintains and complies with a written privacy policy that (a) provides persons with the substantive rights required by the TIPA and (b) "reasonably conforms" to *either* (i) the National Institute of Standards and Technology (NIST)[2] voluntary privacy framework titled "A Tool for Improving Privacy through Enterprise Risk Management Version 1.0" or (ii) "other documented policies, standards and procedures designed to safeguard consumer privacy" (collectively, privacy frameworks). Businesses also have a two-year grace period to "reasonably conform" any written privacy policies to subsequently published revisions of the privacy frameworks to be eligible to utilize this affirmative defense. Notably, the NIST voluntary privacy framework is neither an auditable checklist of actions to perform nor a blueprint of required standards to which to adhere, and the TIPA does not delineate what is necessary or sufficient to "reasonably conform" to applicable privacy frameworks. Accordingly, businesses seemingly have significant flexibility in deciding how to implement and revise their respective written privacy policies.

Under the TIPA, the "scale and scope" of a controller's or processor's privacy program will be assessed based on each of the following five factors: (1) the business size and complexity;

[1] A similar concept was introduced before Ohio's state legislature as part of the Ohio Personal Privacy Act but failed to gain the requisite votes to move forward.

[2] NIST is a nonregulatory agency of the U.S. Department of Commerce tasked with promoting U.S. innovation and industrial competitiveness.

(2) the nature and scope of activity; (3) the sensitivity of the processed personal information; (4) the cost and availability of tools to improve privacy protections and data governance; and (5) compliance with a comparable state or federal law. The open-ended nature of this provision means that, aside from implementing any mandatory obligations, the approaches that businesses take to comply with the TIPA will widely vary, as well as the level of data privacy and protection afforded to consumers considered sufficient to comply with the law.

Privacy Certification as Evidence of Compliance

The TIPA is the first comprehensive state privacy law to expressly recognize certifications under the Asia Pacific Economic Cooperation's Cross-Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP) systems as legally relevant evidence of compliance. Specifically, a controller's CBPR certification and a processor's PRP certification may be considered in assessing whether the scale and scope of a controller's or processor's privacy program is appropriate under the TIPA. Although privacy certifications such as CBPR and PRP have been utilized by companies for years to increase their credibility and demonstrate to the public evidence of best practices regarding customers' data privacy and security, no state or federal privacy laws — other than the Children's Online Privacy Protection Act (COPPA) — had previously officially recognized certification schemes as proof of compliance therewith.

Consumer Rights

The TIPA codified the basic tenets of consumer rights found in other state privacy laws and expressly states that any arrangement purporting to waive or limit such rights is contrary to public policy and as such is void and unenforceable.

The TIPA expressly provides that controllers must comply with certain requests from authenticated consumers. Analogous to Colorado and Virginia, if a controller is unable to authenticate a consumer's request to exercise their consumer rights through commercially reasonable efforts, the controller is not obligated to comply with the request. In such circumstances, a controller may, but is not required to, request that the consumer provide additional information that is reasonably necessary for the controller to authenticate their request.

In particular, the TIPA provides that controllers must comply with the following requests from authenticated consumers:

- **Confirmation and access.** Consumers can confirm whether a controller is processing their personal information and request access to such personal information.
- **Correct inaccuracies.** Consumers can request to correct inaccuracies in their personal information, taking into account the nature of, and purpose for processing, such personal information.
- **Deletion.** Consumers can request that any personal information provided by or obtained about such consumer be deleted. However, a controller is not required to delete information that it maintains or uses as aggregate or de-identified data.
- **Portability.** Consumers can obtain a copy of their personal information that they previously provided to the controller in a portable and, to the extent technically feasible, readily usable format that allows such consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means.
- **Opt-out.** Consumers can opt-out of a controller's processing of personal information for purposes of (i) targeted advertising, (ii) the sale of personal information about the consumer and (iii) profiling through solely automated means in furtherance of decisions that produce legal or similarly significant effects concerning such consumer.

The TIPA expressly provides that the foregoing consumer rights do not apply to "pseudonymous data," defined as personal information that cannot be attributed to a specific natural person without the use of additional information. Such information is exempted from these consumer rights, however, only if the additional information required to reidentify the consumer is (i) kept separately and (ii) subject to effective technical and organizational measures that prevent the controller from accessing such information.

As set forth under comprehensive consumer privacy laws in other states (except Iowa), controllers must respond to an authenticated consumer's request to exercise their consumer rights within 45 days. When reasonably necessary and depending on the complexity and number of requests, controllers may extend the response period once by an additional 45 days so long as the requesting consumer is timely and properly notified. Similar to privacy laws in Colorado, Connecticut, Indiana, Iowa and Virginia (but unlike the privacy laws in California and Utah), the TIPA permits consumers to file an appeal if a controller does not honor the consumer's request. In such an event, the controller must notify the requesting consumer and provide instructions as to how to appeal such decision. Although the TIPA does not stipulate a deadline by when a consumer must file an appeal, the law does expressly provide that controllers have 60 days to respond to a submitted appeal. If a consumer's appeal is denied, the controller must provide the consumer with a method to contact the Tennessee attorney general's office to submit a complaint

given that, as further explained below, the TIPA allows only the state's attorney general to enforce the statute and precludes any private right of action.

No Private Right of Action

Consumers are not able to bring private rights of actions, including class action lawsuits, for TIPA violations. Rather, the Tennessee attorney general has the exclusive authority to enforce the TIPA based upon its own inquiry or public complaints. If a controller or processor is notified by the Tennessee attorney general that it is violating the TIPA but fails to cure such violation within 60 days, the attorney general may then seek a declaratory judgment, injunctive relief, monetary damages up to $7,500 per violation (plus treble damages for willful or known violations), reasonable attorney fees and investigative costs, or other relief that a court deems appropriate. Unlike the privacy laws in California, Colorado and Connecticut, the cure right under the TIPA does not sunset (as is the case with Indiana's privacy law, which we discuss further in this mailing).

The TIPA is not an outlier in prohibiting consumers from bringing private rights of actions. In fact, the same limitation is found in all other general state privacy laws with the exception of the California Consumer Privacy Act (CCPA), which permits consumers to bring a private right of action for certain data breach incidents.

Key Takeaways

Many businesses that comply with other comprehensive state privacy laws will likely have many of the TIPA's requirements in place to comply with the law when it goes into effect in 2025. To take advantage of the TIPA's "first-of-its-kind" built-in affirmative defense and other business-friendly safe harbors, businesses that will be subject to the TIPA may want to consider assessing their privacy policies and practices to determine whether they "reasonably conform" to a privacy framework or can be made to do so without great expense and/or applying for or renewing their CBPR and PRP certifications. Notably, it remains to be seen how invoking the TIPA's built-in affirmative defense will work in litigation and if such business-friendly safe harbors will remain unique to the TIPA or if other states will adapt a similar approach in future state-level legislation. While the TIPA appears to be the most business-favorable comprehensive state privacy law to date, it nonetheless further exacerbates the difficulties for businesses to comply with the ever-growing patchwork of state-level privacy legislation.

Return to Table of Contents

Indiana Enacts Consumer Privacy Law

On May 1, 2023, Indiana became the seventh U.S. state to enact a consumer privacy law when Gov. Eric Holcomb the Indiana Consumer Data Protection Act (INCDPA) into law. The Indiana legislation closely tracks other state privacy laws, in particular those of Utah and Virginia, and thus should impose few new obligations on companies that are already in compliance with these or other state privacy laws. The Indiana law is set to take effect on January 1, 2026.

Scope of the INCDPA

Indiana's law applies to any entity in the state that conducts business in Indiana or which, regardless of where it is located, produces products or services targeted at Indiana residents acting only for personal, family or household purposes (consumers) and that, during a given calendar year, either:

- controls or processes personal data of at least 100,000 Indiana consumers; or
- controls or processes personal data of at least 25,000 Indiana consumers and derives 50% or more of its gross revenue from the sale of personal data.

In the INCDPA "personal data" is defined as any information linked or reasonably linkable to an identified or identifiable individual, excluding de-identified, aggregate or publicly available data. The above thresholds for the number of consumers whose personal data is controlled or processed and the percentage of gross revenue derived from the sale of personal data mirror the thresholds included in the privacy laws in Utah and Virginia.

The Indiana law, as in other state privacy laws, carves out exemptions for certain entities or types of data. For example, the INCDPA does not apply to nonprofit organizations and institutions of higher education, nor does it apply to data and entities covered by federal privacy laws, such as the GLBA, HIPAA and Fair Credit Reporting Act. The law also does not apply to employee data or data collected through business-to-business contacts, with California being the only state that covers those categories of residents in its privacy law.

Obligations of Data Controllers and Processors

Under the INDCPA, "controllers" are defined as a person who, alone or jointly with others, determines the purpose and means of processing personal data and are subject to certain obligations. These obligations are similar to those imposed on controllers under other state privacy laws. Among other requirements, controllers must:

- Limit the collection of personal data to what is adequate, relevant and reasonably necessary in relation to disclosed purposes for which such data is processed. Unless controllers obtain consumer consent, they may not process personal data for purposes that are not reasonably necessary nor compatible with the disclosed purposes for which the personal data is processed.
- Provide a "reasonably accessible, clear, and meaningful" privacy notice to consumers disclosing, among other things, the categories of personal data processed, the purpose of such processing, how consumers can exercise their rights and categories of personal data shared with (*i.e.*, disclosed to) third parties.
- Establish, implement and maintain reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity and accessibility of personal data.
- Clearly disclose if the controller "sells" (defined as "the exchange of personal data for monetary consideration by a controller to a third party") consumers' personal data to third parties or engages in targeted advertising (defined as "displaying of an advertisement to a consumer in which the advertisement is selected based on personal data obtained from that consumer's activities over time and across nonaffiliated websites or online applications to predict the consumer's preferences or interests") and provide consumers an opportunity to opt out. These definitions mirror those in the privacy laws of Utah and Virginia.
- Establish a process by which consumers can appeal the controller's decision not to act on a consumer's request.
- Conduct a data protection impact assessment on the processing of personal data for targeted advertising; and the sale of personal data, profiling, sensitive data and any processing activities that involve personal data that present a heightened risk of harm to consumers. This applies to processing activities are generated on or after January 1, 2026.

The law also imposes requirements on a personal data "processor," which is defined as a person or company that processes personal data on behalf of controllers. For example, processors must assist the controller in meeting the controller's obligations in relation to responding to consumer requests and maintaining the security of processing personal data. All processing must be governed by a written contract between the controller and processor that clearly sets forth instructions for processing personal data, the nature and purpose of processing, the type of personal data subject to processing, the duration of processing, and the rights and obligations of both parties.

Consumer Rights

The Indiana privacy law provides Indiana consumers with the following rights, which mirror those afforded to consumers as part of other states' privacy laws:

- **The right to access.** Consumers can confirm their personal data has been collected by controllers and request access to such data once a year.
- **The right to data portability.** Unlike other state privacy laws, the Indiana law allows covered entities responding to an access request to provide either a complete copy of the personal data provided by the consumer or a representative summary of that data in a portable and, to the extent technically practicable, readily usable format.
- **The right to correct.** Consumers have the right to correct inaccuracies in the personal data previously provided to a controller. Note this right is narrower in scope than the laws of California, Colorado, Connecticut and Virginia, all of which extend this consumer right to all personal data in the possession of the controller.
- **The right to delete.** Consumers have the right to request the deletion of any personal data provided by or obtained about the consumer.
- **The right to opt out.** As in the laws in California, Iowa and Utah, consumers have the right to opt out of the processing of their personal data for purposes of targeted advertising, the sale of personal data and profiling (if done through solely automated means) in furtherance of decisions that produce legal or similarly significant effects concerning that consumer. Note that this right does not extend to pseudonymous data, so long as the controller is able to demonstrate that any information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing such information.
- **The right to opt in.** As required in the privacy laws in Colorado, Connecticut and Virginia, if an Indiana consumer, or a parent on behalf of a child user known to be under the age of 13, does not provide their consent, a controller cannot process their "sensitive data." This data is defined as a category of personal data that includes: (i) personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis made by a health care provider, sexual orientation, citizenship or immigration status; (ii) genetic and biometric data that identifies an individual; (iii) precise geolocation data; or (iv) any personal data collected from a known person under the age of 13. Note that only health information where a diagnosis has been made by a health care provider is considered sensitive data.

No Private Right of Action

The Indiana law does not provide a private right of action, and only the state's attorney general has enforcement authority. Before bringing an enforcement action, the state attorney general must notify controllers or processors of alleged violations and allow them a 30-day cure period, which does not sunset (unlike the sunsetting cure periods in California, Colorado and Connecticut laws). Controllers or processors that violate the INCDPA after this cure period may be subject to an injunction and civil penalties of up to $7,500 per violation.

Key Takeaways

Since the Indiana Consumer Data Protection Act is modeled after other state privacy laws, the legislation likely does not introduce new burdensome obligations on businesses that are already in compliance with such laws. However, companies that will be subject to the INCDPA and do not yet have privacy compliance programs will need to develop and implement such a program before January 1, 2026.

Return to Table of Contents

European Court of Justice Issues Three Key GDPR Rulings

On May 4, 2023, three judgments were handed down by the Court of Justice of the European Union (CJEU) relating to the interpretation of the General Data Protection Regulation (GDPR). The judgments involve key areas of the GDPR, including data subject rights, compensation and the accountability principle. While none of the judgements signal a significant departure from established positions, they do demonstrate that the CJEU continues to take a principle-driven approach to the GDPR and interpret provisions broadly, to the extent possible.

Right of Access to Personal Data by Data Subjects

Summary

In Case C-487/21, the CJEU was asked to determine whether, in response to a data subject access request, the data controller could satisfy the requirement under Article 15 of the GDPR to provide a "copy of the personal data undergoing processing" by providing a list summarizing the data subject's personal data processed by the controller.

The CJEU determined that the right to obtain a "copy of the personal data undergoing processing" means that a data subject is entitled to be given a "faithful and intelligible reproduction" of the personal data being processed. This means that a data subject does have the right to obtain copies of extracts from documents or databases, or entire documents if appropriate, provided that such a copy is required for a data subject to be able to verify that their personal data is correct and has been processed in a lawful manner. The CJEU further confirmed that a data subject must receive a copy of their personal data laid out in a concise, transparent, intelligent and easily accessible form, as per data subjects' rights under the GDPR.

As an example, the CJEU highlighted situations where personal data is generated from other data or where data is generated on the basis of a lack of information (for example, conclusions are drawn from the fact that certain information has not been provided by a data subject). In such situations, the court noted the context in which the data is processed is an essential element in enabling the data subject to have transparent access and an intelligible presentation of their personal data.

In all such situations, the CJEU noted that a balance will have to be struck between a data subject's rights under the GDPR and the rights of others in relation to their personal data when responding to a data subject's request. The result of this balancing measure, however, should not be a refusal by the data controller to provide all of the information to the data subject.

Key Takeaways

Data controllers should be aware that the rights afforded to data subjects in the context of a data subject access requests are broad, meaning data controllers may need to provide additional contextual information to data subjects where necessary and, depending on the request, ensure the requestor receives their information in a transparent and intelligible way.

Compensation Under Article 82 of the GDPR

Summary

In Case C-300/21, the CJEU was asked to determine whether a claimant was entitled to compensation under the GDPR for nonmaterial damage caused by statistical extrapolation of the claimant's personal data, which determined his political affiliation. Notably, the data was not shared with third parties.

The CJEU confirmed that the test for compensation under the GDPR requires that both (i) an infringement of the GDPR and (ii) damage caused by the infringement have occurred. The CJEU recognized that it is therefore possible for an infringement

of the GDPR to occur but not give rise to compensation if there was no damage or no causal link between the infringement and the damage.

The CJEU also confirmed that, as long as both parts of the test stated above are met, there is no threshold that must be met under the GDPR for the seriousness of the damage. Thus, nonmaterial damage (*e.g.*, distress or loss of reputation) could trigger a right to compensation if it was caused by an infringement of the GDPR.

The CJEU noted that the legal systems of member states should determine the detailed rules for calculation of compensation, meaning that the actual compensation received may vary between member states. However, the compensation received should be full and effective, as required under EU law.

Key Takeaways

While this ruling makes clear that a causal link is required between an infringement of the GDPR and any damage suffered, the judgment confirms that no threshold of seriousness is required for damages to give rise to compensation under the GDPR. Going forward, this ruling may cause an increase in the number of claims for compensation where the damage suffered is minor or where there is no financial loss.

The Accountability Principle (Article 5 of the GDPR)

Summary

Case C-60/22 involved the processing and sharing of personal data by state agencies in Germany in the context of judicial proceedings, with the claimants alleging that the state agencies had not processed personal data in compliance with the GDPR. Specifically, the allegation stated certain agencies did not, as required under the GDPR, maintain records of processing activities or conclude a joint controller agreement. The key question before the CJEU was whether these shortcomings were a breach of the accountability principle and amounted to unlawful processing of personal data under the GDPR and, accordingly, whether the data subject was entitled to exercise their right to erasure or restriction of such processing.

The CJEU held that the data controller's failure to comply with the above specific GDPR requirements did not necessarily amount to unlawful processing, which is defined under the GDPR as occurring where there is no lawful basis for processing personal data, amounting to breach of the accountability principle. While a failure to maintain records of processing activities or conclude a joint controller agreement may occur in the context of unlawful processing, such failures do not, by themselves, constitute unlawful processing, the court ruled. Thus, going forward such failures will not entitle a data subject to exercise the rights to erasure or restriction of processing unless there also is no lawful basis for processing.

Key Takeaways

This judgment reaffirms the importance of a key requirement under the GDPR for data controllers to ensure they have a lawful basis for processing. The ruling also emphasizes the importance of the core principles of the GDPR, such as purpose limitation, data minimization, accuracy, storage limitation, and integrity and confidentiality. Data controllers are responsible for compliance with these principles, and have an obligation under the GDPR to be able to demonstrate such compliance.

Return to Table of Contents

California Privacy Protection Agency Announces Potential Regulation Proposals During May Board Meeting

On May 15, 2023, the California Privacy Protection Agency (CPPA) held a board of directors meeting to discuss various updates to certain of its plans and initiatives, including the CPPA's approach to drafting certain potential regulation proposals and updates on new CPRA rules.

Background

The California Privacy Rights Act (CPRA) established the CPPA, which directs the rulemaking process to implement the CPRA's provisions. The CPPA has full administrative authority to enforce both the CCPA and the CPRA[3] (which amended the CCPA) by bringing enforcement actions before an administrative law judge, with the CPPA board meeting regularly to discuss various agency initiatives, updates and priorities. Two of the agency's board meetings held throughout the year are considered rulemaking meetings to discuss proposed regulations and priorities, which was the focus of the May 15, 2023, meeting.

Regulation Proposals and Priorities

One of the topics discussed at the meeting was the CPPA's approach to its regulation proposal process. The CPPA board discussed a high-level list of potential future rules, broken out by ease of implementation, that the CPPA staff may draft for the board to review in future rulemaking meetings.[4] At the meeting, a member of the CPPA noted that agency staff would be able

[3] Enforcement of the CPRA will begin July 1, 2023.

[4] The agenda item containing the list can be found here under Agenda Item 7.

to implement all of the items categorized as "easy" or "easy to medium" by the next rulemaking meeting. The staff requested that the board give authorization to the staff to begin working on such proposed regulation and to provide input on the topics that should be prioritized.

The meeting also provided a chance to understand each board member's rulemaking priorities. One board member noted that the proposed regulation regarding providing template or standard forms for services provider or contractor contracts (Article 4) and providing model notices and other disclosures (Article 2), while likely helpful to the industry, are not currently priorities. Other board members noted that the following should be considered priorities:

- including a reading standard for disclosures and other provisions that make disclosures more accessible (7003);
- considering whether employment-related communications that occur during a person's employment at a business falls within the "trade secret" exception (Business-to-Business Data); and
- considering whether any exceptions or specific rules should apply to employee data (Employee Data).

Nevertheless, the board decided to delegate authority to the CPPA staff by motion to proceed to develop rulemaking proposals on all "easy" and "easy to medium" topics and any other topics in the chart that — in the staff's discretion/judgment, taking into account resources and timing — should be prioritized. The board noted that the staff should take into account the board's preferences as discussed above. However, the staff has ultimate discretion on timing and authority to decide priorities. The CPPA staff will update the board on the status of all items on the list at the next board meeting.

New CPRA Rules Subcommittee Update and Next Steps

The board received an update from the its CPRA Rules subcommittee. The CPPA previously released an invitation for public comments on CPRA proposed regulations for cybersecurity audits, risk assessments and automated decision-making. That comment period has since closed and the CPPA received numerous comments.[5] Accordingly, CPPA staff is processing such comments and are using it to draft proposed language for these rules. The subcommittee noted it will identify key issues for these rules for the board's input at the next board meeting.

Key Takeaways

The CPPA is expected to begin drafting and discussing the proposed regulation topics considered at the board meeting. The agency also will begin discussing key issues for proposed regulations related to cybersecurity audits, risk assessments and automated decision-making. We will continue to monitor the CPPA's activity in the coming months.

Return to Table of Contents

Furniture Company Files Coverage Action Against Crime Insurer After Sustaining Wire Fraud Losses

Furniture company Arnold's Office Furniture, LLC (AOF) has filed a lawsuit against its crime insurer, the Cincinnati Insurance Company (Cincinnati), in the U.S. District Court for the Eastern District of Pennsylvania seeking social engineering fraud coverage for a series of wire fraud losses totaling over $1 million, for which Cincinnati denied coverage.[6]

The Policy's 'Social Engineering Fraud' Coverage

According to the complaint, in January 2021 AOF procured an insurance policy from Cincinnati that included a "Social Engineering Fraud" endorsement. That endorsement covered "loss resulting directly from your having, in good faith, paid, or delivered money, securities or other property in reliance upon a transfer instruction purportedly issued by your customer or vendor, but which transfer instruction proves to have been fraudulently issued by an imposter without the knowledge or consent of your employee." The policy defined the terms "customer" and "vendor" respectively as "an entity or individual to whom you sell goods or provide services under a pre-existing agreement that is still in effect at the time of loss or damage" and "an entity or individual from whom you have purchased goods or received services under a pre-existing agreement that is still in effect at the time of loss or damage."

The Fraudulent Transfers and Losses

AOF alleges that a few months after purchasing the policy from Cincinnati, the company fell victim to a series of fraudulent transactions for which AOF made claims under the policy. Cincinnati subsequently denied all of AOF's claims.

The first incident allegedly arose in April 2021, when an individual posing as an employee of ASR Healthcare contacted AOF to

[5] The public comments can be accessed here.

[6] The case is *Arnold's Office Furniture, LLC v. Cincinnati Insurance Company*, No. 2:23-cv-01581 (E.D. Pa. April 26, 2023).

purchase 200 chairs for $50,000. AOF alleges that after various exchanges, it waived the 75% deposit it typically requires and sent the chairs to the address provided by the individual with a request for payment in 30 days. After multiple attempts to collect payment, AOF allegedly contacted ASR Healthcare by phone, only to learn that AOF had been duped — the actual ASR Healthcare did not authorize the purchase of chairs, did not issue a purchase order to AOF and did not have knowledge of chairs being delivered. AOF alleges that it subsequently filed a police report and submitted a claim to Cincinnati under the policy's Social Engineering Fraud endorsement. Cincinnati denied the claim because AOF did not have a preexisting agreement with ASR Healthcare at the time of the loss, and therefore ASR Healthcare did not qualify as a "customer" under the policy.

In July 2021, AOF submitted another claim to Cincinnati seeking coverage under the policy's Social Engineering Fraud endorsement for a $27,400 loss that AOF incurred when it was tricked into wiring money to a Thailand-based company named Easy Rich Mining Co. for an order of nitrile gloves that AOF never received. Cincinnati denied the company's claim because AOF "had no prior relationship with Easy Rich" before it transferred the funds, and therefore Easy Rich did not qualify as a "vendor" under the policy.

Finally, in April 2022, AOF alleges that it submitted three claims to Cincinnati: one for $183,750, one for $144,000 and another for $658,350. Attempting to secure orders of nitrile gloves, AOF allegedly paid these amounts to cyber criminals posing as legitimate foreign businesses. Cincinnati denied coverage for the claims, once again on the basis that because AOF had no preexisting relationships with the companies at the time of the transactions, they did not meet the policy's definition of "vendors."

AOF's Coverage Action Against Cincinnati

Thereafter, on April 26, 2023, AOF filed a complaint against Cincinnati in the U.S. District Court for the Eastern District of Pennsylvania for breach of contract, statutory and common law bad faith, violation of the Pennsylvania Unfair Trade Practice and Consumer Protection Law and fraud. AOF seeks damages in excess of $150,000 along with compensatory, punitive and treble damages, attorneys' fees, interest and any other relief that the court deems proper. As of the date of the publication of this mailing, Cincinnati had yet to file a response to AOF's complaint.

Key Takeaways

It remains to be seen how the case will be resolved. However, AOF's series of fraudulent transfer losses underscores the importance of employing appropriate safeguards and exercising caution before transferring funds, especially when transacting with companies where no preexisting commercial relationship exists. From an insurance perspective, this case also serves as an important reminder to carefully review the terms of insurance policies when procuring coverage.

Return to Table of Contents

Professional Liability Insurer Seeks Declaration Stating It Does Not Owe Coverage to Attorney for Claims Arising From Hacking Incidents

Professional liability insurer National Liability & Fire Insurance Company (National Liability) has filed an action in Connecticut Superior Court seeking a declaratory judgment that the company does not owe coverage under professional liability policies issued to its insured, real estate attorney William Gouveia, for claims arising out of several incidents in which cyber criminals hacked Mr. Gouviea's computer and altered real estate transaction payment instructions.[7]

The Insurance Policies

According to the complaint, Mr. Gouveia, a Connecticut-based real estate attorney, purchased two substantively identical Lawyers Professional Liability insurance policies from National Liability with claims reporting periods of January 7, 2022, to January 7, 2023, (the 2022 Policy) and January 7, 2023, to January 7, 2024, (the 2023 Policy).

The policies allegedly cover any claim arising "from an act, error or omission in the performance of legal services by [an insured] on behalf of Named Insured or any predecessor firm." The policies define "legal services" as "services provided to others by an Insured in the capacity as . . . [a]n attorney or notary public . . . but only if such services are performed as a member of, or on behalf of, the Named Insured." The policies also contain various exclusions, including for: (1) "the destruction, diminution in value or loss of any property or asset, accounts, or of software, data or other information in electronic form" (exclusions 2.g and 2.f of the 2022 and 2023 Policies, respectively); (2) "[t]he loss or destruction, or any diminution in the value of any asset in your care, custody or control, or out of the misappropriation of, or failure to give an account of, any asset in your care, custody or control, including the commingling of funds" (exclusions 2.n and 2.l of the 2022 and 2023 Policies, respectively) and (3) "[y]our failure to implement, update and maintain commonly accepted

[7] The case is *National Liability & Fire Insurance Company v. Gouveia, et al.*, (Super. Ct. Conn. Hartford Jud. Dist. April 25, 2023).

technologies" (exclusions 2.o and 2.m of the 2022 and 2023 Policies, respectively).

The Hacking Incidents and Mr. Gouveia's Insurance Claim

National Liability alleges that in May and June 2022, hackers obtained access to Mr. Gouveia's computer and "altered payoff instructions for a number of residential real estate transactions" that he handled. In certain of the transactions, Mr. Gouveia allegedly disbursed funds from his trust account based on fraudulent payment instructions. In another, he allegedly directed the disbursement of funds by another attorney based on the fraudulent payment instructions. According to the complaint, the fraudulent transfers have resulted in litigation against Mr. Gouveia by his clients and other individuals involved in the subject transactions.

Mr. Gouveia allegedly sought coverage for the claims under the policies, which National Liability denied.

National Liability Seeks a Declaration of No Coverage

In April 2023, National Liability filed an action in Connecticut Superior Court against Mr. Gouveia and each of the parties involved in the four fraudulent transactions, seeking declaratory relief. In the four-count complaint, National Liability seeks declarations that it has no duty to defend and/or indemnify Mr. Gouveia under the policies with respect to the claims arising out of the fraudulent transfers. National Liability alleges that the claims do not fall within the policies' coverage grant because, in each instance, the claims do not arise from Mr. Gouveia's rendition of "legal services"; rather, each claim arises from his "administrative failure to secure his computer system and/or the ministerial task of instructing another attorney to disburse funds."

National Liability also asserts that exclusions bar coverage for Mr. Gouveia's claims. According to the complaint, exclusions 2.g/2.f preclude coverage because the funds at issue in each transaction are assets that were lost; exclusions 2.n/2.l preclude coverage because the funds at issue "were lost while Gouveia exercised control over them by directing how they should be disbursed"; and exclusions 2.o/2.m preclude coverage because each claim "arises out of Gouveia's failure to implement, update, and/or maintain commonly accepted technologies."

Key Takeaways

This case highlights that cyber thieves continue to target legal services providers with increasing frequency. Particularly given that attorneys and other such professionals often handle financial and other sensitive information, the maintenance of state-of-the-art technologies and safeguards to guard against cyberattacks, such as those allegedly suffered by Mr. Gouveia, is of paramount importance. The case also serves as a reminder that issuers of traditional insurance coverage lines, such as professional liability, may dispute coverage for crime and cyber-related losses, and that coverage typically will turn on the precise wording of the policy.

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

Patrick Fitzgerald
Partner / Chicago
312.407.0508
patrick.fitzgerald@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

Rich 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

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