Skadden

Privacy & Cybersecurity Update

The GDPR at the One Year Mark: A Work in Progress

On May 25, 2018, the EU General Data Protection Regulation (GDPR) went into effect, causing uncertainty regarding the volume and nature of enforcement, with many organizations fearing a shift toward more frequent and aggressive fines. However, following its first anniversary, the reality of GDPR is significantly more nuanced.

The first year of GDPR implementation has met mixed reviews. While there have been some clear developments among data protection regimes, the heavily anticipated level of sweeping enforcement activity has yet to materialize. While enforcement has, by many accounts, lagged expectations, entities, whether they be "data controllers" or "data processors," are taking steps to adapt to the GDPR's new requirements. Additionally, the European Data Protection Board (EDPB) and national supervisory authorities are putting effort into releasing regular guidance and creating tools to assist companies with compliance in their day-to-day practices.

The GDPR also has played an important role in increasing individual awareness of data protection. The European Commission's March 2019 Eurobarometer survey of approximately 27,000 European citizens showed that around 67 percent of those surveyed know what the GDPR is. The Eurobarometer survey also reported that 73 percent have heard of at least one of the six rights guaranteed by the GDPR, while 57 percent indicated they know there is a public authority in their country responsible for protecting their data rights (compared to 2015's survey, in which only 37 percent were aware).

Internationally, the GDPR may start to appear as less of an outlier in data enforcement. Brazil has enacted the Brazilian Data Protection Law (which takes effect August 2020), and other countries, including India and China, are considering similar legislation. In the U.S., the California Consumer Privacy Act (CCPA) (which takes effect January 2020) imposes requirements that are similar to those included in the GDPR.

Data Breach Notifications and Enforcement Actions

The GDPR mandates data breach notifications when personal data an entity is responsible for is accidentally or unlawfully disclosed. Since May 25, 2018, there have been 89,271 data breaches logged by European Economic Area (EEA) supervisory authorities. Of those, 63 percent have been closed and 37 percent are ongoing. The

Netherlands, Germany and the United Kingdom have reported the highest numbers of breaches, with the U.K. Information Commissioner's Office (ICO) noting that it has logged more than 14,000 data breaches (a marked increase over the roughly 3,300 notifications it received in the preceding year). There have been 144,376 queries and complaints — primarily concerning promotional emails, telemarketing and video surveillance, or CCTV — from individuals in the EU since the GDPR's implementation, with 41,000 of those coming from the U.K. and 6,000 from Ireland.

Additionally, GDPR enforcement is still evolving. As of May 22, 2019, there were over 280,000 cases pending investigation across 27 EEA countries. The Data Protection Commission (DPC) in Ireland, a country with a large tech hub, is currently investigating 18 "large data breaches, systemic privacy issues and other serious violations at technology firms," but actions have not yet been taken.

As of February 2019, only 91 fines had been imposed under the GDPR. Total fines have reached €56 million, but the majority of that figure stems from the single €50 million fine levied against Google by the French supervisory authority, Commission Nationale de l'Informatique et des Libertés (CNIL) (Google is currently challenging this action). Prior to its implementation, privacy advocates had expected more accountability and higher levels of enforcement under the GDPR's comprehensive reforms. That said, the U.K. ICO and the Irish DPC publicly have hinted that enforcement actions under the GDPR will be coming in the next few months, but that cases take time to build.

The enforcement actions taken by EEA Supervisory Authorities thus far span a variety of industries and entities, signaling that GDPR fines and enforcement notices will not be reserved for big tech firms or major breaches, as evidenced below by some of the first enforcement actions at a national level:

- On May 28, 2019, the Belgian Data Protection Authority fined a Belgian mayor €2,000 for the use of personal data that initially was collected for local administration purposes in an electoral campaign.
- On July 17, 2018, the first GDPR fine in Portugal was levied against Centro Hospitalar Barreiro Montijo. The Portuguese data protection authority fined the hospital €400,000 for allowing indiscriminate access to personal data, alongside other violations of basic principles of processing, the absence of adequate technical and organizational measures, and inability to ensure continued confidentiality.
- On April 4, 2019, the Italian Data Protection Authority issued a €50,000 fine against the Rosseau internet platform for a number of privacy security issues related to data controlled by Italian political party Movimento 5 Stelle.
- As of May 22, 2019, German regional data protection authorities had imposed a total of €449,000 in fines, including in November 2018, in which a €20,000 fine was levied against a chat and dating service for a breach in which hackers stole 300,000 customers' personal data. The service notified the relevant authority about the breach and an investigation uncovered a lack of appropriate technical safeguards for the protection of data by storing its users' passwords in unencrypted plain text.
- On April 4, 2019, the U.K. ICO issued a preliminary enforcement notice against Her Majesty's Revenue and Customs (HMRC) for the biometric data processed in their Voice ID system. The ICO found that HMRC had given customers insufficient information about the data processing and did not give them a chance to consent. The U.K. ICO's first enforcement notice under the GDPR was levied in October 24, 2018, against AggregateIQ Data Services Ltd, a Canadian company targeting EEA data subjects, for processing personal data without the data subjects' knowledge, as well as for undeclared purposes and without a lawful basis. In both cases, the ICO demanded data deletion as a precursor to imposing a fine.

Looking Ahead and Key Takeaways

While 25 EU member states have adopted national legislation for implementing the GDPR, Greece, Slovenia and Portugal have yet to put their domestic laws in place. Organizations also have called for more clarity on specific elements of the law, including details around data breach notifications and subject rights requests.

As simple cases give way to more complex cases, there are more regulatory questions that will require resolution. For example, there are concerns that individuals, such as former employees, may use data subject rights as punitive measures against companies or to obtain pre-litigation disclosure. In addition, as increasing volumes of personal data are processed in cross-border investigations, the eDiscovery process — and other statutorily or treaty-enabled production requirements, such as those contemplated under the U.S. Clarifying Lawful Overseas Use of Data Act, or CLOUD Act — will require the EDPB and supervisory authorities to be clear about the GDPR's scope, as well as require investigators and companies to be more attentive to the GDPR's requirements.

At the one year mark, there is no doubt that the GDPR has set standards through which legislators and citizens around the world are becoming more aware of their governments' abilities to protect individual rights.

Return to Table of Contents

Nevada Enacts Right to Opt Out of Sale of Information

A new Nevada law requires website operators to offer consumers the ability to request that their personal information not be sold to data brokers.

On May 29, 2019, Nevada enacted Senate Bill 220 (the Nevada Amendment),[1] which amends the Nevada Internet Privacy Act to require "operators" to establish a designated email address, toll-free telephone number or website through which consumers can make a verified request that their covered information not be sold. A verified request means the operator has verified the authenticity of the opt-out request and the identity of the consumer "using commercially reasonable means."

An "operator" is broadly defined as a person who:

- owns or operates a website or online service for commercial purposes;
- collects and maintains certain items of personally identifiable information from consumers who reside in Nevada *and* use or visit the website or online service; and
- engages in any activity that constitutes a sufficient nexus with Nevada to satisfy constitutional requirements. Such activity includes doing business in Nevada, purposefully directing activities toward Nevada or transacting with the state or a Nevada resident.

Certain entities are exempt from the definition of "operator," including, among others, financial institutions and entities subject to certain federal privacy laws. These entities include any entity regulated by the Gramm-Leach-Bliley Act or Health Insurance Portability and Accountability Act (HIPAA), any service provider to an operator, and certain manufacturers of a motor vehicle or persons who service motor vehicles who process covered information.

A "sale" for purpose of the Nevada Amendment is "the exchange of covered information for monetary consideration by the operator to a person for the person to license or sell the covered information to additional persons," unless the information is disclosed for purposes consistent with a consumer's reasonable expectations.

"Covered information" refers to any one or more of the following data points about a consumer collected by an operator through a website or online service: first and last name, street name and name of city or town, email address, telephone number, Social Security number, an identifier permitting a specific person to be contacted, and/or any other information about a consumer collected from that consumer through the website or online service of the operator and maintained in combination with an identifier that makes the information personally identifiable.

Operators must respond to consumers' requests within 60 days. A 30-day extension is available if "reasonably necessary" and notice has been provided to the consumer. An operator that has received a verified request submitted by a consumer must not make any sale of any covered information the operator has collected or will collect about that consumer.

The attorney general may bring a legal action against an operator who violates the Nevada Amendment and can seek an injunction or civil penalty of up to $5,000 for each violation.

California Consumer Privacy Act

Although some have been quick to compare the Nevada Amendment to a comparable provision in the California Consumer Privacy Act (CCPA), there are some critical differences between the two states' approaches.

First, the Nevada Amendment defines "sale" more narrowly than the CCPA, effectively limiting it to the sale (for monetary consideration) to data brokers. The CCPA includes any type of consideration and the "sale" to any other person, not just data brokers. Consumers also are defined more narrowly in the Nevada Amendment than under the CCPA in that employee and business data is not included, although the definition is broad enough to include what most businesses care about (*i.e.*, consumers purchasing goods or services). That said, the Nevada Amendment does not carve out smaller businesses the way the CCPA does. In addition, "covered information" is more narrowly defined under the Nevada Amendment, excluding some of the broad areas picked up by the CCPA, such as device identifiers or household information. Finally, in contrast to the CCPA,

[1] The full text of the bill can be read here.

the Nevada Amendment does not require a business to provide clear and conspicuous notice to consumers of their opt-out right regarding the sale of their information.

Key Takeaways

Overall, the Nevada Amendment is a prime example of the growing reality that, in the absence of federal privacy legislation, companies will be forced to comply with a patchwork of inconsistent state law obligations.

Return to Table of Contents

Maine Restricts Sale of Personal Information by ISPs

A new Maine law requires internet service providers (ISPs) in the state to obtain customer consent before using, disclosing or selling their personal information.

On June 30, 2019, Maine enacted An Act to Protect the Privacy of Online Customer Information (the Maine Act).[2] The Maine Act, which goes into effect July 1, 2020, will ban, subject to certain exceptions, ISPs in Maine from "using, disclosing, selling or permitting access to customer personal information unless the customer expressly consents to that use, disclosure, sale or access." Instead of providing customers the right to opt out of utilization of their data, the Maine Act restricts ISPs from using customers' data unless they have affirmative customer consent. It also requires ISPs to provide "clear, conspicuous and nondeceptive" notice of customer rights and ISP obligations. Additionally, the act requires that ISPs take "reasonable measures" to protect customer information from unauthorized use, disclosure or access when implementing security measures.

"Customer personal information" restricted from sale refers to:

- personally identifiable information about the customer including, but not limited to, the customer's name, billing information, Social Security number, billing address and demographic data; and
- information from a customer's use of broadband internet access service including, but not limited to, the customer's search history, application usage history, precise geolocation information, financial information, health information, IP address, communications contents and information pertaining to the customer's children.

A customer may revoke consent to use, disclose, sell or permit access to customer personal information at any time. As well, a provider may not refuse to serve a customer who does not provide such consent, nor may a provider charge a customer a penalty or offer a customer a discount, based on a decision to provide or withhold such consent.

Among other exceptions, the law states that providers may use, disclose, sell or permit access to customer personal information without express, affirmative customer consent to:

- provide the service from which the information is derived;
- advertise or market the provider's communications-related services to the customer;
- comply with a lawful court order;
- initiate, render, bill for and collect payment for broadband internet access service;
- protect users from fraudulent, abusive or unlawful use of or subscription to ISP services; and
- provide geolocation information concerning the customer in connection with certain enumerated emergency situations.

Key Takeaways

With the enactment of the Maine Act, the state's ISPs now face the strictest consumer privacy protections in the country. More importantly, passage of the legislation represents another "one-off" privacy law that will force companies to either adopt different policies for different states or consider each new privacy law the "floor" for what they need to do nationwide. Many expect the new law to be challenged as violating Federal Communications Commission rules or the interstate commerce clause of the Constitution.

Return to Table of Contents

[2] The full text of the bill can be read here.

Oregon Expands Data Breach Notice Law

Oregon updated its data breach notification requirements to improve transparency surrounding data breaches and expand the definition of personal information.

On May 24, 2019, Oregon enacted a new law, SB 864,[3] which amends the Oregon Consumer Identity Theft Protection Act, effective January 1, 2020, and renames it the Oregon Consumer Protection Act (the act). The act now extends existing data breach notification obligations to a "vendor," defined as a person "with which a covered entity contracts to maintain, store, manage, process or otherwise access personal information for the purpose of, or in connection with, providing services to or on behalf of the covered entity." A "covered entity" is defined as a person that "owns, licenses, maintains, stores, manages, collects, processes, acquires or otherwise possesses personal information in the course of the person's business, vocation, occupation or volunteer activities," except with respect to a person who acts solely as a vendor.

A vendor that discovers a security breach or has reason to believe a security breach occurred must (1) notify any contracted covered entities as soon as practicable, but no later than 10 days after discovering (or having reason to believe that) a breach has occurred, and (2) notify the attorney general if a breach or suspected breach involved the personal information of more than 250 consumers or a number of consumers that the vendor could not determine.

The amendment revises the original legislation's definition of "personal information" to include user names or other means of identifying a consumer for purposes of permitting access to the consumer's online account, together with any other method necessary to authenticate the user name or means of identification.

The act also provides that compliance with security measures under federal data security laws (including HIPAA and the Gramm-Leach-Bliley Act) gives covered entities and vendors in alleged violation of the act an affirmative defense regarding information protected under the act, but not protected under federal laws.

Key Takeaways

Oregon joins a number of states which, in recent years, have strengthened their data breach notification obligations. But, as discussed earlier, the growing number of state legislation continues to make it difficult for entities to adhere to the patchwork of cybersecurity rules and legislation that exist in each state jurisdiction, but not at the federal level.

Return to Table of Contents

Fourth Circuit Holds That Dish Network is Liable for Violating Telephone Consumer Protection Act

The U.S. District Court for the Fourth Circuit affirmed a $61 million treble damages award, finding that the National Do Not Call Registry applies to agents, including sales representatives and third-party marketers, under the Telephone Consumer Protection Act (TCPA).

On May 30, 2019, the Fourth Circuit affirmed a district court decision in favor of a certified class, concluding that satellite television company Dish Network (Dish) is liable for the actions of its agent, Satellite Systems Network (SSN), and reaffirmed judgment for approximately 11,000 plaintiffs.[4]

Unlawful Phone Calls

The named plaintiff, Dr. Thomas Krakauer, alleged that he began to receive telemarketing phone calls in May 2009, asking him to buy services from Dish, at a number he had listed in the Do Not Call Registry. The calls were placed by SSN, acting on behalf of Dish. Krakauer called Dish to complain about the calls, and he was placed on the company's individual Do Not Call list. In 2015, Krakauer sued Dish for the improper calls under the TCPA, seeking redress for himself and all persons who objected to these calls.

TCPA Regulations

The TCPA allows a private right of action for violations of the Do Not Call Registry regulations. By its plain language, the TCPA's private right of action contemplates that a company can be held liable for calls made on its behalf, even if not placed by the company directly.

[3] The full text of the amendment can be read here.

[4] *Krakauer v. Dish Network, L.L.C.*, No. 18-1518 (4th Cir. May 30, 2019).

The District Court Finds Liability and Willful Violations

In September 2015, the court certified a class that closely followed the text of the TCPA, allowing Krakauer to bring his claim on behalf of all persons (1) whose numbers were on the National Do Not Call Registry or the individual Do Not Call lists of either Dish or SSN for at least 30 days and (2) received two calls in a single year. The case went to trial, and the jury returned a verdict in favor of Krakauer and the class plaintiffs, finding that the telemarketing practices violated the TCPA and that Dish was liable for the calls placed by SSN. The jury awarded damages of $400 per call. The district court determined that Dish's violations were willful and knowing, and thus trebled the damages award under the TCPA. Dish appealed, challenging the class certification and its own liability for the wrongful calls placed by SSN.

The Fourth Circuit Affirms

The Fourth Circuit affirmed the class certification, ruling that the class was harmed under the TCPA by receiving unwarranted phone calls from SSN, acting as a third-party marketer for Dish. The court rejected all three issues that Dish raised on appeal. First, the court rejected Dish's argument that the members lacked standing because their injury did not rise to "a level that would support a common law cause of action" based on *Spokeo, Inc. v. Robins*,[5] which explains "the traditional core of standing" is a personal stake in the case. The court found that receiving unwanted calls on multiple occasions is an intrusion of personal privacy, and therefore, the members had standing.

Second, the court held the class was properly certified as a matter of civil procedure. Under Rule 23 and the remedial purpose of the TCPA, the cause of action allows for "resolution of issues without extensive individual complications." Dish's contention that the class definition was overbroad was rejected, as the court found the TCPA's cause of action for violations of the Do Not Call Registry can be brought by any "consumer," not only "subscribers."

Finally, the court affirmed the jury's conclusion that SSN was acting as Dish's agent at the time it made the improper calls. The evidence supporting an agency relationship was considerable, including suggestive contract provisions, authorization to use Dish's name and logo to carry out business operations, and the Voluntary Compliance Agreement that Dish entered into with 46 state attorneys general, wherein Dish clearly stated its authority over SSN with regard to TCPA compliance. Although Dish contended that its contract with SSN expressly disavowed an agency relationship, the court found that parties cannot avoid legal obligations of agency by contracting out of them. Dish also asserted it should not be responsible for SSN's actions because it occasionally instructed SSN to follow the law, and, therefore, no reasonable jury could conclude the calls were made within the scope of SSN's authority as Dish's agent. The court found that the jury appropriately resolved this question, concluding that the evidence showed Dish failed to address these concerns in any meaningful way and was profiting from the SSN sales tactics. Accordingly, the court concluded that "this case demonstrates the need to look beyond the contract, as a failure to do so might lead to absolving a company, like Dish, that acquiesced in and benefitted from a wrongful course of conduct that was carried out on its behalf."

Key Takeaways

As the court's decision in *Krakauer* illustrates, TCPA plaintiffs are not required to show any threshold level of injury to have standing if they are able to prove the statutory elements of a TCPA claim, which could possibly lead to an increase in such claims. The Fourth Circuit's decision also may lead to claims involving instances where third parties were used to conduct telemarketing activities.

Return to Table of Contents

Sixth Circuit Holds Payment Processing Company Liable for Damages Related to Attack on Merchant's Credit Card System

On June 7, 2019, the Sixth Circuit affirmed[6] a district court ruling in favor of Spec's Family Partners, a chain of liquor stores in Texas, finding that First Data Merchant Services, the payment processing company used by Spec's, must bear the costs stemming from two attacks on the payment card network used by the stores.

Attacks on Payment Card System and Cost-Shifting Chain Reaction

Spec's Family Partners fell victim to two attacks on its payment card network in which malware was installed to access customer data. An investigation revealed that Spec's failed to comply with the Payment Card Industry Data Security Standard (PCI DSS) prior to the attacks, which left it vulnerable to breaches in its customers' data security.

[5] 136 S. Ct. 1540 (2016).

[6] *Spec's Family Partners, Ltd. v. First Data Merchant Services LLC* No. 17-5884/5950, 2019 WL 2407306 (6th Cir. June 7, 2019).

The attacks, and subsequent data theft, triggered a cost-shifting reaction down the credit card chain. The banks that issued the compromised credit cards first reimbursed the defrauded cardholders and replaced their customers' credit cards. Card brands Visa and Mastercard then issued assessments on the acquiring bank, Citicorp Payment Services Inc., to cover its costs. Third, Citicorp demanded payment from First Data to cover the costs imposed on Citicorp by the credit card companies. Finally, First Data sought reimbursement for those costs from Spec's.

In order to recoup its costs, First Data withheld the proceeds of routine payment card transactions from Spec's, placing the proceeds in a reserve account. Spec's refused to pay First Data and filed suit in an attempt to recover the $6.2 million that First Data withheld.

District Court Grants Summary Judgment

The District Court for the Western District of Tennessee granted summary judgment in favor of Spec's, holding that First Data materially breached the Merchant Agreement when it diverted funds to reimburse itself for the card brand assessments. Specifically, the court found that such assessments constituted consequential damages that could not be recovered under a limitation of liability clause in the First Data contract. The District Court refused to interpret the assessments as "third-party fees and charges," for which Spec's would be liable under the contract.

Sixth Circuit Affirms

The Sixth Circuit reviewed *de novo* the grant of summary judgment and affirmed the District Court ruling in its entirety. First Data argued on appeal that Spec's was liable for the assessments under the contract's indemnification clause and because they constituted "third-party fees and charges" under the agreement.

The Sixth Circuit rejected First Data's indemnity argument, finding that the assessments passed down to First Data constituted consequential damages because, according to Tennessee law, consequential damages are the natural consequences of the act complained of, but not the necessary results of such conduct. In other words, the assessments constituted consequential damages because the data breaches, reimbursements to cardholders and levying of assessments were the natural results of PCI DSS non-compliance. However, the results were not a necessary consequence of non-compliance in the sense that a non-compliant merchant might never suffer a data breach and the card brands might not issue assessments in the case of PCI DSS non-compliance on its own. The court concluded that because the data breaches and the imposition of assessments did not necessarily follow from the actions of Spec's, the losses sustained were consequential and Spec's could not be held liable for such damages under the contract.

First Data also argued that Spec's was liable under a provision in the contract stating that Spec's was responsible for all "third-party fees and charges" associated with the use of First Data's services. By looking to the ordinary and plain meaning of the term, as well as its meaning within the context of the entire agreement, the Sixth Circuit held that the term "third-party fees and charges" did not include or contemplate assessments imposed by credit card companies. The court also noted that the only other federal appeals court to address this exact issue reached the same conclusion that the term excludes assessments following a data breach.[7]

Finally, the Sixth Circuit affirmed the District Court's ruling that First Data materially breached the agreement by withholding payments due to Spec's. The Sixth Circuit found that the PCI DSS non-compliance was an immaterial breach that was cured when Spec's took steps to achieve full compliance. The court concluded that First Data materially breached the agreement by withholding payments due to Spec's and thereby deprived Spec's of the principal expected benefit under the contract.

Return to Table of Contents

New Guidance Clarifies Direct Liability of Business Associates Under HIPAA

In late May 2019, the Department of Health and Human Services (HHS) Office for Civil Rights released guidance regarding business associate liability under HIPAA and the Health Information Technology for Economic and Clinical Health Act (HITECH).

In 2013, HHS issued a rule, under the HITECH Act, that made business associates directly liable for certain HIPAA-related violations. However, since its enactment, the scope and reach of the rule has been unclear. On May 24, 2019, the Office of Civil Rights issued a fact sheet to clarify the rule, listing 10 provisions of HIPAA for which business associates can be held directly liable.

[7] *Schnuck Markets, Inc. v. First Data Merchant Services*, 852 F.3d 732 (8th Cir. 2017)

The HHS guidance will clarify matters regarding business associates, which include consultants, billing companies and medical record providers, among others. Though HIPAA applies directly to health care providers, plans and clearinghouses, certain vendors qualify as business associates if they handle protected health information (PHI) on behalf of, or in providing services to, a HIPAA-covered entity.

The 10 provisions under which business associates will be held liable are:

1. Failure to provide the HHS secretary with records and compliance reports; cooperate with complaint investigations and compliance reviews; and permit access by the secretary to information, including PHI, pertinent to determining compliance.
2. Taking any retaliatory action against any individual for filing a HIPAA complaint; participating in a retaliatory investigation or other enforcement process; or opposing an act or practice that is unlawful under the HIPAA rules.
3. Failure to comply with the requirements of the HIPAA Security Rule (which includes the risk analysis requirement).
4. Failure to provide breach notification to a covered entity or another business associate as required by the HIPAA Breach Notification Rule.
5. Impermissible uses and disclosures of PHI.
6. Failure to disclose a copy of electronic PHI to either the covered entity, the individual or the individual's designee (whichever is specified in the business associate agreement) to satisfy a covered entity's obligations regarding the form and format, as well as the time and manner, of access.
7. Failure to make reasonable efforts to limit PHI to the minimum extent necessary to accomplish the intended purpose of the use, disclosure or request.
8. Failure, in certain circumstances, to provide an accounting of disclosures.
9. Failure to enter into business associate agreements with subcontractors that create or receive PHI on their behalf, and failure to comply with the implementation specifications for such agreements.
10. Failure to take reasonable steps to address a material breach or violation of the subcontractor's business associate agreement.

Key Takeaways

The new guidance clarifies uncertainty regarding when and how business associates can be held directly liable for HIPAA violations. In addition to liability imposed by the Office for Civil Rights, a business associate should be aware of contractual commitments regarding the handling of PHI imposed by covered entities.

Return to Table of Contents

European Council Approves New EU Cybersecurity Act

The newly passed EU Cybersecurity Act intends to combat the increasing risks of cyberattacks as they become more sophisticated and, more frequently, international. The Cybersecurity Act aims to prompt a coordinated and collaborative response across the EU.

Background

On June 7, 2019, the European Council formally approved Regulation (EU) 2019/881 (the Cybersecurity Act), which came into force on June 27, 2019. The Cybersecurity Act enacts two principal measures: (1) strengthens the role of the European Union Agency for Network and Information and Security (ENISA), the EU agency that improves network and information security in the EU and (2) introduces the first EU-wide cybersecurity certification framework. For now, the single certification framework will be voluntary rather than compulsory, with the goal of building a harmonized framework for uniform cybersecurity standards across the EU. The introduction of the Cybersecurity Act will not, therefore, necessarily prompt immediate action, but demonstrates the EU's cybersecurity focus and gives a framework for manufacturers and service providers of information and communications technology (ICT) products, services and processes to be mindful of.

The Ever-Expanding Role and Powers of ENISA

The Cybersecurity Act strengthens ENISA by granting a permanent mandate and strengthening its human element. ENISA has been a temporary EU agency since its establishment in 2004. While ENISA is not a regulatory authority, it enhances cybersecurity prevention work by advising the European Commission, analyzing data and raising awareness on potential cyber threats.

With the Cybersecurity Act, ENISA's role expands through the supervision and facilitation of information sharing across the EU. ENISA also will now maintain a website providing information on cybersecurity, including the certification framework.

Additionally, ENISA will now assist with designing certification schemes for ICT products and services. At a foundational level, these schemes will ensure that key cybersecurity standards are adhered to by ICT manufacturers and service providers, such as by ensuring an adequate level of protection of personal data against unauthorized storage, processing, destruction, exfiltration, loss or alteration. ENISA also is tasked with reviewing certification schemes every five years to ensure their ongoing compliance with adequate cybersecurity standards.

Certification Framework

The Cybersecurity Act establishes an EU cybersecurity certification framework that aims to assure consumers of the safety of their data, allowing them to trust the cybersecurity of ICT products, services and processes. The framework also provides a uniform certification process in the EU, avoiding multiple, conflicting and overlapping certifications between countries. The ENISA certification schemes will be based on European or international cybersecurity standards, though they will be supervised and implemented by national authorities. EU member states also may establish individual national penalties for infringing the schemes.

It is expected that the first ENISA certification scheme will be published within a year of the Cybersecurity Act's effective date. The Cybersecurity Act grants the European Commission the power to decide whether to adopt the published ENISA certification schemes. The European Commission also will re-evaluate, by 2023, whether some schemes should be mandatory. As such, it will take time to conclude whether the Cybersecurity Act is successful and whether the certification regime will become an effective, trusted and useful exercise for ICT providers and manufacturers, as well as consumers.

Relationship With Other Data Protection and Cybersecurity Laws

The Cybersecurity Act dovetails closely with other European Union laws addressing data protection and cybersecurity, most notably the GDPR, which requires technical and organizational measures to safeguard the processing of personal data, and the Network and Information Security Directive (NIS Directive), which was the first EU-wide legislation on cybersecurity and addresses potential cybersecurity threats against network and information systems. However, the Cybersecurity Act differs in that its purview extends beyond the NIS directive, which only applies to businesses classified as "operators of essential services" and "digital service providers," whereas the Cybersecurity Act extends to all manufacturers and service providers of ICT offerings.

Key Takeaways

The Cybersecurity Act's true impact and efficacy remain to be seen. However, the increased focus on cybersecurity issues could facilitate the successful and widespread adoption of ENISA certification schemes. Cybersecurity has been a high priority for both businesses and the EU in recent years, and the Cybersecurity Act, if nothing else, reinforces the importance of strong cybersecurity standards.

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

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

David Eisman
Partner / Los Angeles
213.687.5381
david.eisman@skadden.com

Patrick Fitzgerald
Partner / Chicago
312.407.0508
patrick.fitzgerald@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

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

Amy Park
Partner / Palo Alto
650.470.4511
amy.park@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

Ivan Schlager
Partner / Washington, D.C.
202.371.7810
ivan.schlager@skadden.com

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

Jen Spaziano
Partner / Washington, D.C.
202.371.7872
jen.spaziano@skadden.com

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

Donald L. Vieira
Partner / Washington, D.C.
202.371.7124
donald.vieira@skadden.com

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

Jessica N. Cohen
Counsel / New York
212.735.2793
jessica.cohen@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
Four Times Square
New York, NY 10036
212.735.3000