June 2021

Skadden

Privacy & Cybersecurity Update

European Commission Publishes New Standard Contractual Clauses

On June 4, 2021, the European Commission (EC) published a new set of Standard Contractual Clauses (SCCs) for the transfer of personal data outside of the European Economic Area (EEA).

The transfer of personal data outside of the EEA has been a topic of significant contention and a source of great uncertainty for organizations following the Court of Justice of the European Union (CJEU) decision in July 2020 in *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems (Schrems II)*, which invalidated the EU-U.S. Privacy Shield as a data transfer mechanism. The SCCs remained valid subject to enhanced due diligence on the part of both the data exporter and data importer to ensure that the privacy laws of the importing country were adequate. Since *Schrems II*, the European Data Protection Board (EDPB) has issued guidance on what such due diligence should cover, including in relation to the assessment of the laws of third countries and the supplementary measures the parties should implement if the laws fall short of the required standard. The EDPB recommendations on the supplementary measures was finalized on June 18, 2021, and we have summarized that guidance below.

New SCCs: Key Features

The new SCCs now align with the General Data Protection Regulation (GDPR) and further seek to address the issues around governmental access to personal data identified by the CJEU in *Schrems II*. This is a much-needed update, as the old set of SCCs were designed for and referenced the previous data protection legal framework, the Data Protection Directive 1995/46/EC. The new SCCs reflect the reality of modern data transfers by accounting for four types of transfers:

- **Controller-to-Controller SCCs**. As with the old SCCs, these are to be used for transfers from controllers within the territorial scope of the GDPR to controllers in a third country (*i.e.*, any countries outside the EEA that have not received to date an adequacy decision from the European Commission, which states that the country's national legal framework ensures an adequate level of protection of personal data).
- **Controller-to-Processor SCCs**. As with the old SCCs, these are to be used for transfers from controllers within the territorial scope of the GDPR to processors in a third country. This type of SCC now includes the mandatory Article 28 GDPR data processing

provisions, meaning that parties no longer need to enter into a separate data processing addendum (DPA). Where parties have entered into a DPA and now execute the new controller-to-processor SCCs, the terms of the new controller-to-processor SCCs will prevail over the terms of the former DPA.

- **Processor-to-Controller SCCs**. This type of SCC is for transfers from processors within the territorial scope of the GDPR to controllers in a third country.
- **Processor-to-Processor SCCs**. This type of SCC is for transfers from processors within the territorial scope of the GDPR to their processors or sub-processors in a third country and also includes the mandatory Article 28 GDPR data processing provisions, meaning that parties need not enter into a separate DPA.

While controller-to-controller and controller-to-processor SCCs are updated versions of the old SCCs, the processor-to-controller and processor-to-processor SCCs are the first of their kind.

In addition, rather than four entirely separate SCCs, the EC has adopted a modular approach in which the SCC can be customized to the type of transfer by adding or deleting certain paragraphs. The new SCCs will be a welcome change for processors that use sub-processors outside the EEA or whose controllers are located outside the EEA. Under the old SCCs, such transfers were not accounted for, meaning that parties were left with limited or no options to validly effect such transfers. The introduction of the processor-to-controller and processor-to-processor SCCs means that parties can now cover these transfers. Additionally, the inclusion of the Article 28 GDPR data processing provisions in the controller-to-processor SCCs and processor-to-sub-processor SCCs removes the need for companies to enter into multiple contracts for the same data processing activity, thereby reducing organizations' paperwork burden.

More specifically, the new SCCs include the following key features:

Docking Clause. The new SCCs contain a "docking clause" that allows third parties to subsequently accede to the agreement. This is in contrast to the old set of SCCs that only allowed for bilateral parties. The docking clause czoncept will provide greater flexibility to organizations, particularly in intra-group scenarios, and will limit the need for companies to enter into numerous separate contracts. For example, if organizations wanted to add a newly incorporated or acquired entity to the prior SCCs, they would either have had to enter into a separate set of SCCs or sign a deed of accession allowing the new party to accede to the SCCs. Under the new SCCs, this process is now more streamlined.

Geographic Scope. The old SCCs were only an appropriate transfer mechanism in cases where the data exporter was located in the EEA. The new SCCs, however, acknowledge that data exporters could actually be located outside the EEA while sitting within the territorial scope of the GDPR (*e.g.*, data exporters that provide goods or services to individuals in the EEA, thereby satisfying the "targeting criterion" in Article 3.2 of the GDPR). Furthermore, Recital 7 of the new SCCs provides that the SCCs need not be implemented when both the data exporter and data importer are within the territorial scope of the GDPR and are accordingly subject to GDPR requirements. Although we are still at the very early stages of the introduction of the new SCCs, and absent further guidance to date from the EC and EDPB to this effect, it remains to be seen whether organizations will proceed without the new SCCs when subject to GDPR requirements yet based outside the EEA. In practice, it may be the case that organizations will remain cautious and adopt a risk-adverse approach by implementing nevertheless the new SCCs to safeguard such transfers.

- ***Schrems II* Provisions**. The CJEU's decision in *Schrems II* left many companies questioning how to comply with the GDPR for data transfers to third countries (particularly the U.S.). The new SCCs have a dedicated section addressing the *Schrems II* ruling that requires parties to warrant that they have no reason to believe that the local laws and practices of the destination jurisdiction will result in the data importer being unable to adhere to its obligations under the SCCs. The parties also would then need to complete a documented assessment in providing this warranty, considering (a) the specific circumstances of the transfer; (b) the laws and practices of the third country of destination, including those requiring the disclosure of data to public authorities or authorising access by such authorities; and (c) any relevant contractual, technical or organizational safeguards put in place to supplement the safeguards under the SCCs. This documented transfer assessment also aligns with the GDPR accountability principle and will need to be shared with the relevant supervisory authority on request. In practice, we expect that large-scale data importers in third countries will seek to attract customers (who are the data exporters) by performing transfer assessments on their behalf. In other instances, we expect that data exporters will perform such assessments in-house or engage consultants or law firms to assist.
- **Enforcement of the New SCCs**. The new SCCs require that data importers located in third countries submit to the competency and jurisdiction of the data exporter's supervisory authority and courts. Where the data exporter is not established in the EEA, the competent supervisory authority and courts will be that of the place of establishment of the

European representative. Additionally, by entering into the new SCCs the data importer agrees to cooperate, respond to any inquiries, submit to any audits undertaken by, and comply with any requests issued by, the competent supervisory authority. The new SCCs therefore create a stronger nexus between a non-EEA data controller and European supervisory authorities.

Individuals Rights Reinforced. The new SCCs reinforce data subjects' rights by enabling them to receive a copy of the new SCCs, request information about the relevant processing operations subject to the transfer, contact controllers located outside the EEA and obtain compensation for any damages that they may suffer as a result of such transfer.

Timing of Compliance

The new SCCs became effective on June 27, 2021. Additionally:

- Until September 26, 2021, organizations have the option of choosing whether to rely on the old SCCs or the new SCCs to safeguard their transfers.
- Thereafter, on September 27, 2021, the old SCCs will be repealed and will no longer be a valid data transfer mechanism for *new* data transfers. Companies already relying on the old SCCs at that time will then have until December 26, 2022, to transition to the new SCCs.
- Starting on December 27, 2022, the old SCCs will not be valid for any data transfers. Although organizations will inevitably need to spend a significant amount of time and resources re-papering their data transfer relationships, the transition period will allow organizations to do this gradually over time.
  - Organizations participating in short-term projects which are likely to have concluded by December 27, 2022, can choose to enter into the old SCCs until September 27, 2021.
  - However, organizations engaging in long-term projects that are likely to continue beyond December 27, 2022, should consider using the new SCCs to avoid an unnecessary re-papering exercise.

It is important to remember that the new SCCs apply to transfers outside the EEA and not the U.K. In May 2021, the U.K. Information Commissioner's Office (ICO) confirmed that it was working on its own set of SCCs. As such, it will be interesting to see the extent to which the ICO's own set of SCCs, due to be published next month, may differ from the EC's new set of SCCs.

In the meantime, organizations should start planning and getting ready to implement the new SCCs ahead of the December 27, 2022, cutoff date.

Return to Table of Contents

Post-*Schrems II*: European Data Protection Board Issues Final Recommendations on International Data Flows

On June 18, 2021, the EDPB issued the final version of its recommendations on supplementary measures for the compliant and safeguarded transfers of personal data outside of the EEA.[1] The recommendations seek to address comments received during the period of public consultation following the EDPB's initial draft published in November 2020 (the draft recommendations). Although the recommendations retain the requirement for organizations to complete an extensive transfer impact assessment before transferring data to third countries, there are a number of key changes between the two versions that are summarized below.

Background

The GDPR requires that parties implement a valid data transfer mechanism for the transfer of personal data out of the EEA to any country that has not received an adequacy decision from the European Commission. Only Andorra, Argentina, Canada, the Faroe Islands, Guernsey, Israel, the Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the U.K. have been issued adequacy decisions to date.

The CJEU decision in the *Schrems II* case invalidated the EU-U.S. Privacy Shield for data transfers to the U.S. and imposed enhanced due diligence requirements on parties relying on SCCs as a data transfer mechanism. The CJEU stipulated that where such enhanced due diligence determines that the importing country's laws do not provide a level of protection "essentially equivalent" to that in the EEA, supplementary measures must be implemented by the parties. Our November 2020 *Privacy & Cybersecurity Update* (accessible here) outlined the main features of the draft recommendations issued by the EDPB in relation to such supplementary measures, particularly regarding the transfer impact assessment that organizations should undertake before transferring data outside the EEA using one of the GDPR Article 46 data transfer mechanisms (including Binding Corporate Rules).

EDPB Updated Guidance: Key Differences

The newly issued recommendations build on the draft recommendations by taking into account feedback received during the public consultation period and aligning with the new set of SCCs published by the EC. However, the recommendations do retain

[1] The full text of the recommendations can be accessed here.

the same structure as the draft recommendations by outlining a six-step roadmap for organizations to follow before transferring data to third countries. In completing this assessment, data exporters must take into account all of the actors participating in the transfer, including controllers, processors, sub-processors and any onward transfers.

The key differences and updates from the draft recommendations include:

- **Practices of Third Countries and Third Country Public Authorities**. The language of the recommendations in relation to Step 3, in which exporters must: "assess whether the Article 46 GDPR transfer tool you are relying on is effective in light of all circumstances of the transfer" contains a subtle but important difference from the draft recommendations. It states that a data exporter must assess if there is anything "in the law and/or practices in force in the third country" where the data is being transferred (including, specifically, the practices of public authorities) that may impinge on the effectiveness of the safeguards in being relied on for the transfer. This aligns with the language in Clause 14 of the new SCCs, which similarly specifies that the parties should consider the laws and practices of the destination country together. Organizations should therefore be mindful to look not only at the black letter law in the importing country, but also at the practices of third countries (including the practices of the data importer) and third country public authorities in determining whether the transfer is sufficiently safeguarded. Specifically, an extra step must be undertaken in the transfer assessment to consider whether public authorities of the third country (a) may seek to access the data with or without the data importer's knowledge, in light of legislation, practice and reported precedents, and (b) may be able to access the data through the data importer, telecommunication providers or communication channels in light of legislation, legal powers, technical, financial and human resources at their disposal and of reported precedents. However, if the assessment concludes that the requirements or powers of public authorities "restrict the fundamental rights of data subjects while respecting their essence and being necessary and proportionate," they may not automatically be considered to impinge on the effectiveness of the Article 46 GDPR transfer mechanism.
- **Problematic Legislation in Third Countries**. Where a transfer assessment reveals that the third country's legislation is "problematic," data exporters now have the option to (a) suspend the transfer, (b) implement supplementary measures to prevent the risk of the transfer or, notably, (c) proceed with the transfer without supplementary measures if there is no reason to believe that the problematic legislation will be applied in practice to the transferred data or the data importer. Although this will give organizations more flexibility in determining how to proceed with transfers going forward, companies should be mindful that choosing option (c) requires a documented, detailed report outlining how and why the problematic legislation will not be applied in practice.
- **Scope of Laws and/or Practices in Third Countries**. Organizations will be relieved to know that the recommendations have narrowed the scope of the assessment required by the data exporter, limiting it to legislation and practices "relevant to the protection of the specific data you transfer." Consequently, it will be unnecessary for data exporters to carry out general or all-encompassing assessments unless, as explicitly stated in the recommendations, the relevant rules and practices being considered generally have an impact on the effective application of the safeguards contained in the GDPR Article 46 transfer tool.
- **Sources of Information**. The onus is on the data importer to provide the data exporter with all sources of information relating to the destination country that are relevant to the transfer assessment. The recommendations stipulate that these sources should be "relevant, objective, reliable, verifiable and publicly available." Accordingly, the list of sources in Annex 3 has been expanded from the draft recommendations to include, among others, (a) reports based on practical experience with prior instances of requests for disclosure from public authorities, (b) warrant canaries of the importer and (c) reports from private providers of business intelligence. Organizations should note that this list in Annex 3 is non-exhaustive.
- **Derogations**. Although the draft recommendations acknowledged that the derogations contained in GDPR Article 49 should be used restrictively (in an occasional and non-repetitive manner), the recommendations go slightly further than this. They explicitly emphasize that the derogations should be interpreted such that they do not "contradict the very nature of the derogations as being exceptions from the rule." Organizations must therefore only turn to the derogations in extremely specific and limited situations, and should seek to rely on alternative avenues for transferring data in the first instance.

Use Cases

The recommendations contain a number of use cases, which provide practical examples and outline scenarios where the EDPB cannot envisage an effective technical measure being put in place.

For example, Use Case 7 discusses the transfer of personal data for business purposes, including by way of remote access. The example discusses a situation where the data in question is not or cannot be pseudonymized or encrypted because the processing requires accessing the data in the clear (for example, in an intragroup or joint venture relationship). The EDPB outlined three aspects of a scenario where the organization would be incapable of envisioning an effective technical measure to prevent access from infringing on the data subject's fundamental rights:

- A data exporter transfers personal data to a third country by making it available in an information system in a way that allows the data importer direct access to data of its choice, or by transferring it directly, individually or in bulk through the use of a communication service;
- The data importer (whether a controller or processor) processes the data in the clear in the third country; and
- The power granted to public authorities of the third country to access the data goes beyond what is necessary and proportionate in a democratic society, where problematic legislation of the third country applies to the transfer in question.

Companies should therefore be mindful of all factors that the EDPB will consider relevant in relation to data transfers, including technical measures, organizational measures, and the laws and practices of the third country.

Key Takeaways

The EDPB has made some key changes to the recommendations since November 2020, some of which will provide welcome clarification for organizations, while others will require companies to put in additional time and resources to complete transfer impact assessments. The six-step assessment, as well as the implementation of the new set of SCCs, will be burdensome and time-consuming for many organizations, but will endeavor to protect and enhance the fundamental rights of data subjects following *Schrems II* by embodying the GDPR principles of accountability and transparency.

Return to Table of Contents

White House Releases Statement Advising on Steps To Protect Against the Threat of Ransomware

The Biden administration has recommended that private sector companies take precautionary measures to prevent ransomware threats and cyberattacks, releasing an open letter to business executives urging them to step up protections.

The Biden administration has recommended that private sector companies take precautionary measures to prevent ransomware threats and cyberattacks, releasing an open letter to business executives urging them to step up protections.

Introduction

In recent months, there has been a marked increase in ransomware attacks across various American sectors, spanning from the oil and meat industries to government agencies. Ransomware attacks occur when hackers use a set of tools to access computer systems, subsequently locking or disrupting computer functionalities through encryption until the hackers receive a monetary payment. In some cases, hackers may exfiltrate information and data from a targeted company and destroy such data upon a ransomware payment. According to some security experts, the increase in attacks is likely due in part to rise of remote work during the pandemic, which has exposed major cybersecurity vulnerabilities. Relatedly, the U.S. Department of Justice declared the year 2020 to be the "worst year" for cyberattacks connected to extortion[2]. Additionally, in 2021, ransomware attacks have increased by over 100% in comparison to the start of the previous year.[3]

The White House's Response

The U.S. government is increasing its efforts to address ransomware threats and is encouraging cooperation from the private sector to mitigate the risk of future attacks. As such, on June 2, 2021, Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger released an open letter to corporate executives and business leaders urging them to adopt protective measures.

The letter outlines the Biden administration's efforts to deter hackers, including by disrupting ransomware networks, working with international partners to hold countries that harbor ransomware actors accountable, developing policies for ransom payments, and enabling rapid tracing and interdiction of virtual currency proceeds. The letter also states that "companies that view ransomware as a threat to their core business operations rather than a simple risk of data theft will react and recover more effectively."[4]

The letter offers a number of recommended steps, starting with adopting the federal government's "five best practices," as outlined in President Joe Biden's "Executive Order on Improving the Nation's Cybersecurity":

1. **Multifactor authentication**, in which a user is granted access only after effectively presenting two or more pieces of evidence to an authentication tool;

[2] See *The Wall Street Journal*'s April 21, 2021, article "Ransomware Targeted by New Justice Department Task Force."

[3] See Check Point's May 12, 2021, blog post "The New Ransomware Threat: Triple Extortion."

[4] See the White House open letter "What We Urge You To Do to Protect Against the Threat of Ransomware."

2. **Endpoint detection**, a security solution that monitors and collects activity data from endpoints that may indicate a threat;
3. **Endpoint response**, an automatic removal or containment of identified threats after detection with prompt notification to security personnel;
4. **Encryption**, the process of encoding information to render it unintelligible if intercepted; and
5. **Security teams**, a group of personnel with the capability to patch rapidly, as well as share and incorporate information in a company's defense.

In addition to these practices, the White House memo urges corporate executives and business leaders to (1) back up company data, system images and configurations, while regularly testing them and storing the backups offline; (2) update and patch systems promptly; (3) test incident response plans; (4) check the work of security teams; and (5) segment networks. Additional resources in the memo include a fact sheet of President Biden's executive order to improve U.S. cybersecurity and protect federal government networks as well as the Cybersecurity & Infrastructure Security Agency's (CISA) ransomware and guidance resources, discussed below.

Federal Guidance on Ransomware

In September 2020, CISA and the Multi-State Information Sharing and Analysis Center released a joint *Ransomware Guide* that included industry best practices and a response checklist that may serve as a ransomware-specific addendum to an organization's cyber incident response plans. CISA also published a fact sheet for critical infrastructure owners that provides information on the rising risk of ransomware to industrial control systems, as well as recommended actions to reduce risks. The fact sheet also included ways to reduce severe business or functional degradation after a ransomware attack.

CISA recommends the following additional practices to mitigate against ransomware:

- avoiding links or opening attachments in unsolicited emails;
- restricting user permissions to install and run software applications by applying the principle of "least privilege" to all systems and services;
- using application allow-listing (whitelists) to allow only approved programs to run on a network;
- enabling strong spam filters to prevent phishing emails from reaching end users and authenticating inbound emails to prevent email spoofing;
- scanning all incoming and outgoing emails to detect threats and filter executable files from reaching end users; and
- configuring firewalls to block access to known malicious IP addresses.

Victims of ransomware are encouraged to immediately report to CISA at www.us-cert. gov/report, or at a local FBI Field Office or Secret Service Field Office.

Key Takeaways

With the rise of ransomware attacks, companies are well-advised to consider the steps recommended in Ms. Neuberger's letter. In addition, companies should be mindful that regulators and potential plaintiffs may look at guidance issued by the federal government as a checklist of what companies should be doing.

Return to Table of Contents

Supreme Court Adopts Narrow Interpretation of Computer Fraud and Abuse Act

On June 3, 2021, the Supreme Court ruled in *Van Buren v. United States* that the Computer Fraud and Abuse Act of 1986 (CFAA) does not apply to all individuals who misuse authorized access to a computer, even if for an improper purpose, but instead applies only to those who exceed their authorized access by obtaining information located in particular files, folders or databases that are off-limits to them.

Background

The CFAA is a federal criminal anti-hacking law that criminalizes the act of accessing computers or computer systems "without authorization" or in a way that "exceeds authorized access."[5] The term "exceeds authorized access" is defined to mean "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[6]

The plaintiff in the case, Nathan Van Buren, a police sergeant at the time, befriended a man named Andrew Albo, who was considered "very volatile," according to the deputy chief of Mr. Van Buren's former police department. Mr. Van Buren asked Mr. Albo for a personal loan and Mr. Albo secretly recorded their conversation, after which he filed a complaint to the local

[5] 18 U. S. C. §1030(a)(2).

[6] 18 U. S. C.§1030(e)(6).

sheriff's office claiming that Mr. Van Buren sought to "shake him down" for money. As a result, the recorded conversation was sent to the FBI, which planned a sting operation to see what length Mr. Van Buren would go to acquire Mr. Albo's money.

As part of the investigation, Mr. Albo asked Mr. Van Buren to search the state law enforcement computer for a license plate number in return for $5,000. Mr. Van Buren knowingly used his patrol-car computer to access the law enforcement database with his credentials and searched the database for the license plate that Mr. Albo had provided, against department policies. After obtaining the FBI-created license plate entry, Mr. Van Buren told Mr. Albo that he had information to share. The federal government then charged Mr. Van Buren with a felony violation of the CFAA on the grounds that running the license plate for Mr. Albo violated the "exceeds authorized access" clause.

The jury convicted Mr. Van Buren, and the district court sentenced him to 18 months in prison. He appealed to the Eleventh Circuit, arguing that the "exceeds authorized access" clause applies only to those who obtain information to which their computer access does not extend, not to those who misused access that they otherwise have. While there is a split in authority regarding the scope of liability under the CFAA, the Eleventh Circuit affirmed Mr. Van Buren's conviction, stating that he had violated the CFAA by accessing the law enforcement database for an "inappropriate reason."

The Supreme Court granted *certiorari* filed by Mr. Van Buren to resolve the split in authority regarding the scope of liability under the CFAA's "exceeds authorized access" clause. The main question was whether a person violates a section of the CFAA if they access the information to which they had appropriate access rights but utilizes the access for an improper purpose.

The Supreme Court's Ruling

In a 6-3 decision authored by Justice Amy Coney Barrett, the Supreme Court overturned the Eleventh Circuit's ruling and held that an individual who uses an authorized computer to access areas of the computer to which they have appropriate access — such as files, folders and databases — does not violate the "exceeds authorized access" clause of the CFAA, even if the individual uses the accessed information for an improper purpose.

The Court analyzed the disputed phrase "entitled so to obtain," which essentially asks whether a person has the right, in "the same manner as has been stated," to obtain the relevant information. Mr. Van Buren argued that the phrase means information one is not allowed to obtain "by using a computer that he is authorized to access," while the government argued that it meant information one was not allowed to obtain "in the particular manner or circumstances in which he obtained it."[7] The Court found Mr. Van Buren's interpretation more plausible than the government's position, stating that the statute's structure supports that interpretation.

The Court also noted that Mr. Van Buren's reading of the "access without authorization" and "exceed[ing] authorized access"[8] places the provisions of the statute in a harmonious whole. Further, the Court explained that Mr. Van Buren's reading calls for a "gates-up-or-down" inquiry, meaning that to violate the CFAA a person needs to bypass a gate that is down that the person isn't supposed to bypass such as "particular areas of the computer — such as files, folders and databases — that are off-limits to him."[9]

Lastly, the Court stated that the government's broad interpretation of the CFAA would attach criminal penalties to a breathtaking amount of commonplace computer activity, which underscores the implausibility of their interpretation.

Key Takeaways

The Court's opinion has nationalized the narrower CFAA interpretation, thereby overruling CFAA precedent in the First, Fifth, Seventh and Eleventh Circuits, and thus "resolving" the circuit split as to what falls under an unauthorized access within the CFAA. Additionally, the Court's ruling has averted a broader reading of the CFAA that could have criminalized commonplace computer activity, such as using work computers to send personal emails or visiting news websites in violation of workplace policies, limiting computer access to business-purpose only.

Return to Table of Contents

Colorado Expected To Become Third State To Adopt Comprehensive Privacy Law

On June 8, 2021, the Colorado state senate passed the Colorado Privacy Act (CPA). If Gov. Jared Polis signs the bill into law as expected, the CPA will take effect on July 1, 2023, and would make Colorado the third state — after California and Virginia — to enact comprehensive data privacy legislation.

If signed into law, CPA would grant Colorado residents (consumers) various data privacy rights and impose obligations on the "controllers" and "processors" of consumers' personal

[7] *Van Buren v. United States*, 593 U. S. ____ (2021).

[8] 18 U. S. C. §1030(a)(2).

[9] *Van Buren v. United States*, 593 U. S. ____ (2021).

information. The rights and duties established by the CPA echo those created by the California Privacy Rights Act of 2020 (CPRA), which amended and expanded the California Consumer Privacy Act of 2018 (CCPA), and Virginia's recently enacted Consumer Data Protection Act (CDPA). However, despite their similarities, the CPA includes important distinctions that will further complicate companies' data privacy compliance efforts in the U.S. Should Gov. Polis sign the bill into law as anticipated, companies that will be subject to the CPA will have approximately two years to evaluate and modify their consumer data collection and usage policies to satisfy their evolving compliance obligations.

Which Businesses Are Covered?

The CPA would apply to entities that conduct business in Colorado and those that conduct business outside of the state but produce commercial products or services intentionally targeted to Colorado residents if they either: (1) control or process the personal data of at least 100,000 Colorado residents per calendar year; or (2) derive revenue from the sale of personal data and control or process the personal data of at least 25,000 Colorado residents.

The scope of Colorado's new privacy law is similar to that of Virginia's regulation. However, the CPA would have broader applicability since Virginia's law imposes an additional condition for the second threshold, requiring that the company derives at least 50% of its gross revenue from the sale of personal data. Like Virginia's CDPA, the Colorado law does not include a revenue trigger, meaning that large entities will only be subject to the CPA if they meet the personal data thresholds. Thus, the CPA's scope is narrower than that of the CCPA and CPRA because California's laws also apply to any business with more than $25 million in annual revenue, regardless of how much personal data it processes.

Exemptions

The CPA also would not apply to data maintained for employment record purposes, and contains several substantive exemptions to applicability that mirror California and Virginia. This includes, for example, certain types of information already governed by the Health Insurance Portability and Accountability Act (HIPAA). However, Virginia's CDPA is distinct from the CPA in that the former includes a carve-out for covered entities or business associates established under HIPAA, even if the personal data at issue is not itself covered by HIPAA. The CPA, on the other hand, only excludes information and documents that are created by covered entities for the specific purpose of complying with HIPAA. The CPA also has an exemption for entities and personal information subject to the Gramm-Leach-Bliley Act (GLBA). This carve-out is similar to that of Virginia's law but distinct from California's laws, which only exclude information and not entities under the GLBA. As with Virginia's law, the CPA would further exempt specific information already regulated by the Fair Credit Reporting Act (FCRA), the Children's Online Privacy Protection Act (COPPA), the Family Educational Rights and Privacy Act (FERPA) and the Driver's Privacy Protection Act. California's laws, in contrast, do not exempt information regulated by COPPA or FERPA.

Which Consumers Are Covered?

A "consumer" is defined under the CPA as "an individual who is a Colorado resident acting only in an individual or household context." Echoing the business-to-business and employment carve-out under Virginia's CDPA, the CPA excludes from its definition of consumer any "individual acting in a commercial or employment context, as a job applicant, or as a beneficiary of someone acting in an employment context." Although California's CPRA contains a similar exemption, that carve-out will become inoperative on January 1, 2023, unless it is extended.

What Information Is Protected by the CPA?

The lynchpin of all privacy laws is the definition of "personal data," which is defined under the CPA as "information that is linked or reasonably linkable to an identified or identifiable individual." This construct is virtually identical to that in Virginia's CDPA, and — like Virginia — does not include specific categories of data that are found in California's CCPA and CPRA. In another distinction from the California laws, the definitions of personal data under the Colorado CPA and Virginia's CDPA do not include information linkable to "households."

Exemptions

As with the laws in California and Virginia, the definition of personal data under Colorado's law explicitly excludes "de-identified data or "publicly available information." Publicly available information under the CPA, as in the other two states, is defined as information that is lawfully made available from government records, and further excludes information that a business "has a reasonable basis to believe the consumer has lawfully made available to the general public."

As with Virginia's law, certain consumer rights under the CPA would not apply to "pseudonymous data" (*i.e.*, personal data that is not attributable to a specific individual without the use of additional information) as long as the controller can demonstrate that the information necessary to identify the consumer is "kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing the information."

Controllers and Processors

As in Virginia, Colorado's CPA utilizes the categories of "controllers" and "processors" to lay out obligations for businesses, mirroring the approach of the EU's GDPR. A controller is defined as any "person that, alone or jointly with others, determines the purposes and means of processing personal data," whereas a processor is any "person that processes personal data on behalf of a controller." A majority of the duties created by the CPA are imposed on controllers rather than processors.

Consumer Rights

As with the California and Virginia laws, the CPA would grant consumers a series of individual data privacy rights, including the rights to opt out, access, deletion, correction and portability. Consumers would be able to exercise the following rights under the CPA by submitting verifiable requests to which controllers must respond within 45 days. A controller may extend the response period by 45 additional days if it provides the consumer with notice within the initial period.

Right To Opt Out

Consumers would have the right to "opt out of the processing of personal data concerning the consumer for purposes of: (a) targeted advertising; (b) the sale of personal data; or (c) profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer." Under the CPA, as with California's laws, a "sale" of personal data would be defined to occur when a controller exchanges a consumer's personal data with a third party for monetary or other valuable consideration. This definition is broader than that of Virginia's CDPA, which defines the "sale of personal data" as the exchange of personal data only for monetary consideration by the controller to a third party. Sales under the CPA would not include disclosures to a third party of personal data as an asset transfer that is part of a merger, acquisition, bankruptcy or other transaction in which the third party assumes control of the controller's assets.

Under the CPA, controllers may provide consumers with the option to consent to the processing of their personal data. However, the controller must provide the user with "a clear and conspicuous notice informing the consumer about the choices available [under the CPA], describing the categories of personal data to be processed and the purposes for which they will be processed, and explaining how and where the consumer may withdraw consent."

Beginning on July 1, 2024, controllers that process personal data for targeted advertising or the sale of personal data would be required to provide consumers with the ability to opt out through a "user-selected universal opt-out mechanism that meets the technical specifications established by the attorney general." This sets Colorado's law apart from the California laws, which make global privacy control optional. Colorado's attorney general must establish rules governing the technical specifications of universal opt-out mechanisms by July 1, 2023.

Right of Access

Consumers have the right to "confirm whether a controller is processing personal data concerning the consumer and to access the consumer's personal data."

Right to Correction

Consumers have the right to "correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data."

Right to Deletion

Consumers have the right to "delete personal data concerning the consumer." This right under Colorado's law is similar to Virginia's but distinct from California's in that it does not include specific exemptions to the right to deletion. Furthermore, while the right to deletion under California's laws only applies to personal data that the business has collected directly from the consumer, the right under the CPA would cover data "concerning" the consumer, ostensibly including personal data provided by third-parties sources. This is similar to the right under Virginia's law, which applies to personal data provided by or "obtained about" the consumer.

Right to Data Portability

When exercising the aforementioned right to access personal data, under the CPA consumers would have the right to "obtain the personal data in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another entity without hindrance." This right would be able to be exercised up to two times per calendar year.

Obligations Imposed on Businesses

The CPA simultaneously would impose limitations on businesses' collection and use of consumers' personal data and requires specific security and transparency measures.

Duty of Transparency

A controller would have to provide consumers with "a reasonably accessible, clear, and meaningful" privacy notice that explains the types of personal data collected or processed by the controller or processor and the purposes for which such data are processed; the types of information the controller shares with third parties; and how and where consumers may exercise their privacy rights.

Duty of Purpose Specification

A controller would be required to "specify the express purposes for which personal data are collected and processed."

Duty of Data Minimization

A controller's collection of personal data must be "adequate, relevant, and limited to what is reasonably necessary in relation to the specified purposes for which the data are processed."

Duty To Avoid Secondary Use

A controller would be prohibited from processing personal data "for purposes that are not reasonably necessary to or compatible with the specified purposes for which the personal data are processed, unless the controller first obtains the consumer's consent."

Duty of Care

A controller would be obligated to "take reasonable measures to secure personal data during both storage and use from unauthorized acquisition" in a way that is "appropriate to the volume, scope, and nature of the personal data processed and the nature of the business."

Duty To Avoid Unlawful Discrimination

A controller would be prohibited from "process[ing] personal data in violation of state or federal laws that prohibit unlawful discrimination against consumers."

Duty Regarding Sensitive Data

A controller would not be allowed to process a consumer's "sensitive data" without first obtaining the consent of the consumer or, in cases involving a known child, without first obtaining consent from the child's parent or lawful guardian. "Sensitive data" under the CPA is defined as "personal data revealing racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, sex life or sexual orientation, or citizenship or citizenship status" as well as "genetic or biometric data that may be processed for the purpose of uniquely identifying an individual" and "personal data from a known child" (*i.e.*, an individual under 13 years of age). Notably, and unlike Virginia's CDPA and California's CPRA, the CPA does not include a consumer's precise geolocation data in its definition of sensitive data.

While both the CPA and Virginia's CDPA require controllers to obtain consumers' affirmative consent to collect or process their sensitive data, California's laws only impose an obligation to provide an opt-out mechanism (unless the sensitive data belongs to a child).

Data Protection Assessments

A controller must conduct a data protection assessment for each of its processing activities involving personal data that present a heightened risk of harm to consumers, such as processing sensitive data, selling personal data and processing personal data for targeted advertising or certain profiling. This requirement is similar to the data protection assessment requirements of Virginia's CDPA. The data protection assessments under both the CPA and CDPA must identify and weigh the benefits of processing the personal data against the risks such processing poses to the rights of the consumer. Controllers also must identify any safeguards that may mitigate such risks.

The Colorado law empowers its attorney general and district attorneys to access and evaluate a controller's data protection assessment — a right granted only to the attorney general in Virginia. Importantly, however, the disclosure of a data protection assessment under the CPA, as with Virginia's CDPA, does not constitute a waiver of any attorney-client privilege. Furthermore, such assessments are confidential and exempt from public inspection under the Colorado Open Records Act.

Data Processors

Data processors would be required to adhere to the instructions of the controller and assist the controller to meet its obligations under the CPA. The CPA requires controllers and processors to enter into a contract that establishes their relationship and respective obligations. Among other duties, processors are obligated to:

- take "appropriate" technical and organizational measures to assist controllers in responding to consumer requests to exercise their rights under the law;
- provide controllers with all information necessary to demonstrate compliance with its obligations;
- provide controllers with all information necessary to conduct and document data protection assessments;
- support controllers in relation to the security of processing personal data and breach notifications; and
- allow for and cooperate with "reasonable" audits and inspections by controllers or controllers' designated auditor, or arrange for a qualified and independent auditor to conduct an audit of the processor's policies and technical organizational measures.

Enforcement

As with Virginia's CDPA but unlike California's CCPA and CPRA, the Colorado law does not create any private right of action for consumers. Instead, Colorado's attorney general and district attorneys would have exclusive authority to enforce the CPA. The Colorado law is commensurate with the California laws and distinct from Virginia's law in that the CPA grants its attorney general the broad authority to promulgate rules for the purpose of carrying out the CPA. Until July 1, 2025, the Colorado attorney general would have the discretion to adopt rules that govern the process of issuing opinion letters and interpretive guidance to develop an operational framework for businesses.

Prior to taking any enforcement action to address noncompliance, the Colorado attorney general or district attorneys must issue a notice of violation to the controller. Upon receiving such notice, the controller would have 60 days to cure the alleged violation. However, it is important to note that this cure period would only be available to controllers until January 1, 2025. The CPA's temporary cure period is double the length of the two other states' data privacy laws. The right to cure under the California and Virginia laws, however, does not set to expire.

Uncured violations of the CPA would be deemed "deceptive trade practices" punishable by civil penalties. Although the CPA does not specify the penalty amounts, civil penalties under the Act would be governed by C.R.S. § 6-1-112 of the Colorado Consumer Protection Act. Under that statute, civil penalties could be up to $20,000 for each violation with a maximum penalty of $500,000 for any related series of violations. In contrast, the Virginia law imposes civil penalties of up to $7,500 for each violation, while the California laws impose a civil penalty of $2,500 for each violation or $7,500 for each intentional violation. The CPRA also imposes a $7,500 penalty for each violation involving a minor.

Key Takeaways

Despite similarities to California's CCPA and CPRA and Virginia's CDPA, the rights and obligations created by Colorado's new privacy law contain enough differences such that companies operating nationally (or at least in these three states) would have at least three distinct data privacy frameworks to contend with. As a result of the laws' subtle yet important distinctions, compliance with one data privacy law would not necessarily ensure compliance with the others. Accordingly, businesses should carefully consider the nuances between the privacy laws of each applicable state to ensure their compliance. Should Gov. Polis sign the bill into law as anticipated, companies that will be subject to the CPA will have approximately two years to evaluate and modify their consumer data collection and usage policies to satisfy their evolving compliance obligations. Companies also will need to decide whether they adopt an omnibus "least common denominator" approach to compliance or handle the privacy of each state's consumers differently. Finally, it is very possible that other states will enact privacy laws that go into effect at or around the same time as the Colorado law.

Return to Table of Contents

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
213.687.5010
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

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

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

This communication is provided by Skadden, Arps, Slate, Meagher & Flom LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This communication is considered advertising under applicable state laws.

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