Skadden

Privacy & Cybersecurity Update

California Privacy Rights Act Passes, Bringing Changes to the California Consumer Privacy Act

California voters passed the California Privacy Rights Act of 2020 (CPRA) on November 3, 2020, with 56% of voters supporting the measure, which includes new privacy protections that supplement existing safeguards under the California Consumer Privacy Act (CCPA).

Less than three months after the finalization of California Attorney General Xavier Becerra's CCPA implementing regulations, California voters opted to enhance their privacy protections with the passage of the CPRA.[1] While the CPRA largely functions to supplement current consumer safeguards provided under the CCPA, it also extends certain compliance exemptions that were set to expire at the end of 2020. Additionally, the passage of the CPRA means that even companies that completed implementation of their California privacy compliance regimes following finalization of the attorney general's guidelines under the CCPA must continue to carefully monitor regulatory developments in California privacy law and prepare to allocate additional resources toward their compliance workstreams.

Background

The passage of the CPRA is the latest development in a push by privacy advocates to increase the rights of California residents over their personal information. In 2018, over 629,000 state residents signed a petition to place an earlier version of the CCPA on the state ballot. Ultimately, this spurred the California legislature to act prior to the 2018 election and pass the version of the CCPA that is in effect today. Following the passage of the CCPA, the California attorney general presented several rounds of proposed regulations in order to further implement and augment the statutory text. Concurrently, sponsors of the original petition — who were unsatisfied with the final version of the CCPA that was passed — added the CPRA to the 2020 state ballot in order to correct what they considered significant deficiencies in the current regulatory scheme.

The CPRA brings five key changes that will take effect imminently, as well as numerous edits to the original CCPA text that will become enforceable in 2023. As discussed below, as in the original CCPA, the CPRA provides for the promulgation of new administrative regulations, meaning the full set of requirements are far from complete.

[1] A copy of the CPRA can be found here.

Key Imminent Changes to Existing Law

The CPRA contains changes in five specific areas that will become effective five days after the certification of the election results by the California secretary of state, which must occur by December 11, 2020:

- **Extension of Business Personnel and Business-to-Business Exemptions.** The CPRA extends, until January 1, 2023, the current exemptions from most requirements under the CCPA for (1) personal information of business personnel (including employees and contractors) and (2) personal information processed in the context of business-to-business communications. Notably, businesses must continue to provide their personnel with a notice prior to collection of personal information that contains (a) the categories of personal information to be collected and (b) purposes for which such information will be used. This will be a welcome extension for businesses that only engage with California residents through business-to-business contacts or as California-based employees.
- **Establishment of the Consumer Privacy Fund.** The CPRA creates the Consumer Privacy Fund, which will be used (1) to offset costs to the state courts in connection with CCPA actions, (2) to support the California attorney general in carrying out its CCPA duties and (3) for certain other enumerated purposes, such as grants to nonprofit organizations related to consumer privacy, to educate children on privacy issues and to fund law enforcement efforts to combat fraud related to consumer data breaches.
- **Creation of the California Privacy Protection Agency (CalPPA).** Among the most significant changes under the CPRA is the establishment and funding of a new state agency to regulate businesses and enforce Californians' privacy rights. Pre-CPRA, privacy advocates argued that the attorney general did not have sufficient resources or focus to adequately enforce the CCPA. The new agency, CalPPA, is "vested with full administrative power, authority, and jurisdiction to implement and enforce the California Consumer Privacy Act" as amended by the CPRA. Initial appointments to the CalPPA board (on which there will be five seats) must be made within 90 days by four separate state officials. CalPPA will have the authority to coordinate with other data protection agencies in California, as well as in other states and countries. Given the number of concepts in the CCPA and CPRA that are similar to those in the EU's General Data Protection Regulation (GDPR), it remains to be seen the extent to which CalPPA will coordinate with European data protection authorities on matters of data privacy.
- **Attorney General To Transfer Regulatory Authority to CalPPA.** Beginning the earlier of (1) July 1, 2021, and (2) six months after CalPPA provides notice to the attorney general that it is prepared to exercise CCPA regulatory authority, the power currently held by the attorney general to adopt regulations under the CCPA will transfer to the CalPPA. The CPRA provides for such regulations to be finalized by July 1, 2022. The California attorney general will retain its authority to enforce the CCPA through civil penalties.
- **Designation of Funds for CalPPA.** The CPRA calls for an initial $5 million from California's general fund for fiscal year 2020 and $10 million per year thereafter to be designated for operation of CalPPA. Since the attorney general had previously requested less than $5 million per year to hire staff for CCPA-related efforts, this enhanced financial allocation suggests that CalPPA will have the resources to develop a more detailed compliance program than was previously contemplated for CCPA enforcement and privacy advocacy.

Other Key Changes Under the CPRA

The rest of the CPRA may be enforced starting January 1, 2023. With the exception of the right of access, the CPRA only applies to personal information collected by a covered business on or after January 1, 2022. Since the CPRA makes dozens of changes to the existing CCPA and CalPPA is not required to finalize the related regulations until July 1, 2022, it will be some time before businesses have a clear understanding of the CPRA's implications for their compliance programs. Some of the notable changes to the CCPA's text that will impact how businesses adapt their privacy compliance efforts include:

- **Definition of Business.** The CRPA modifies the definition of a "business" in ways that may impact the applicability of the CCPA to certain entities, especially where such an entity has several affiliates. For example, the CPRA revises the threshold for buying, selling or sharing personal information of consumers or households from 50,000 to 100,000 to trigger applicability, and "devices" have been removed from consideration. Additionally, the CPRA confirms that commonly controlled affiliates of a qualifying business that share branding, but do not themselves meet the CCPA's requirements, are only subject to the CCPA if the qualifying business shares consumers' personal information with the non-directly qualifying entity.
- **Sensitive Personal Information; Right To Limit Use and Disclosure.** The CPRA creates the new category of "sensitive personal information," which covers data types such as Social

Security numbers, financial account credentials, precise geolocation information, genetic data, biometric information, race and ethnicity, union membership, and information regarding sex life or sexual orientation. The CPRA creates a new right for consumers to direct a business to limit the use and disclosure of such information "to that use which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services." Businesses that use or disclose sensitive personal information beyond this threshold must include a link on their homepage titled "Limit the Use of My Sensitive Personal Information," through which consumers may exercise this right.

- **Data Retention.** The CPRA requires businesses to notify consumers of the length of time it intends to retain each category of personal information (including sensitive personal information) at or prior to the time of collection. In instances where it is not possible to determine this time period, the business may not retain the consumer's personal information for longer than reasonably necessary.
- **Right of Correction.** The CPRA grants consumers a new right to request that a business correct inaccurate personal information that is retained by the business. In order to exercise this right, the business must process a verifiable consumer request.
- **Contracting Requirements With Third Parties.** The CPRA creates a new obligation for businesses to include certain provisions in their contracts with service providers. Such agreements must do the following: (1) specify that the personal information is sold or disclosed by the business only for limited and specified purposes; (2) obligate the service provider to comply with applicable obligations under the CPRA and provide an equivalent level of privacy protection as required under the CPRA; (3) grant the business the right to take reasonable and appropriate steps to help ensure that the service provider uses the personal information in a manner consistent with the business' obligations under the CPRA; (4) require the service provider to notify the business if it makes a determination that it can no longer comply with the CPRA; and (5) grant the business the right to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information.
- **Annual Cybersecurity Audit and Periodic Risk Assessment.** The CPRA requires the issuance of new regulations requiring businesses whose personal information processing "presents significant risk to consumers' privacy or security" to (1) conduct an annual cybersecurity audit and (2) submit to CalPPA on a regular basis (not currently defined) a risk assessment regarding the business's processing of personal information. While the details of such requirements will be defined in the coming months, businesses should ensure their management teams become familiar with these new auditing and reporting requirements in the near future, especially where a business processes sensitive or large volumes of personal information.

Key Takeaways

The passage of the CPRA means California privacy law will continue to evolve significantly in the coming years. Accordingly, businesses must undertake additional analyses and efforts to supplement their California privacy compliance to date. However, despite this evolution, the current CCPA remains in effect and is enforceable until the corresponding provisions under the CPRA become effective (mostly in 2023), meaning it is still important for companies to comply with the existing CCPA. Additionally, pending CalPPA's issuance of regulations under the CPRA, businesses should begin to consider how to incorporate these new requirements into their compliance programs.

Return to Table of Contents

UK's Information Commissioner's Office Publishes Final Guidance on an Individual's Right To Request Data Access

An individual's right to access the personal data an organization holds about them is a fundamental right under the GDPR and the U.K. Data Protection Act 2018. On October 21, 2020, following a lengthy consultation period that began in December 2019, the U.K.'s Information Commissioner's Office (ICO) published its finalized guidance on how organizations should handle such access requests.[2] Given the increase in volume of access requests since the implementation of the GDPR, organizations should familiarize themselves with the guidance to ensure that such requests are handled efficiently, effectively and in line with GDPR time requirements.

Article 15 of the GDPR entitles individuals to obtain from controllers certain information held about them. The right of access, described by the ICO as a "cornerstone of data protection law," allows individuals to verify what personal data controllers

[2] The ICO's guidance can be accessed here.

are processing about them, and whether such processing is lawful. A controller has one month to respond to an individual's access request, but can extend the time to respond by an additional two months if the request is complex or if the controller has received multiple requests from the individual. The guidance addresses certain operational uncertainties that organizations were facing in relation to these access requests, providing clarity for controllers and individuals processing European Economic Area (EEA) personal data.

The Guidance

The guidance sets out the following key points:

- **The "Clock" for Responding to Access Requests is Stopped When the Controller Requests Clarification.** Controllers have one month to respond to an individual's data request. However, where the controller genuinely needs further clarification, or processes a large amount of data about the individual, it can request that the individual specify the information or processing activities to which his or her request relates before responding. The one-month time limit for responding to the access request will pause until the controller receives the further information. The clock will restart on the day that the controller receives the clarification and the original one-month time period will be extended by the number of days the clock had been stopped. For example, if the controller receives an access request on December 7, the clock will start that day, and the response will be due on January 7. If the controller requests clarification on December 10, the clock will stop that day If the requester provides the clarification on December 12, the clock will resume on December 12. In this scenario, the clock was paused from December 10 to December 12, a total of two days. As such, the controller could then extend the original response deadline by two days to January 9.

  This may assist employers who hold large amounts of employee personal data in various formats (*e.g.*, personnel and performance records, emails and other correspondence), allowing them to narrow the request before the clock restarts. When requesting clarification, controllers should explain why the clarification is being sought and that the clock will be stopped until the information is received.
- **Responding to an Access Request May Involve Disclosing the Personal Data of Third Parties.** Under the U.K. Data Protection Act 2018, controllers must not, as part of their response to an access request, disclose information that identifies a third party, except if the third party has consented or if it is reasonable to disclose the information without the individual's consent. This involves a balancing exercise that weighs the data protection rights of the individual making the request against the rights of the third party. The assessment of whether it is reasonable to disclose the information without the third party's consent should take into account all of the relevant circumstances, including the type of information that would be disclosed, any duty of confidentiality owed to the third party, and whether it is possible to obtain the third party's consent.
- **Whether a Request is "Complex" for the Purposes of a Time Limit Extension Will Depend on the Context.** To determine if a request is complex, the guidance notes that the controller's circumstances, as well as the nature of the request itself, should be taken into account. In relation to the controller's circumstances, a large multinational corporation with thousands of employees and sophisticated internal systems is more likely to be able to handle a complex access request than a startup with limited employees and resources. In relation to the request itself, controllers should consider the technical difficulties in retrieving the data (*e.g.*, is it stored digitally or on a hard copy), any specialist work it will have to carry out to ensure the data is presented in an intelligible manner, and whether the request involves a large amount of data (although the guidance clarifies that a request should not be considered complex merely because of the amount).
- **Controllers Can Refuse To Comply With Manifestly Excessive or Unfounded Requests.** This has always been the case, but the guidance offers more detail on when these exemptions may be applicable:
  - A request may be manifestly excessive if it is "clearly or obviously unreasonable," based on whether the request is proportionate when balanced against the burden of complying with it. For example, if an employee who has been employed by a small local business for 20 years requests access to all of their personal data, much of which is in hard copy and stored at an off-site storage facility, the employer could argue that it is "clearly or obviously unreasonable," to comply with the request, taking into account the costs to the employer of locating and retrieving the relevant personal data, and the volume of personal data. However, the guidance is clear that the assessment must be done on a case-by-case basis and controllers should not have blanket policies in place.

- A request may be manifestly unfounded if the individual "clearly has no intention" to exercise their right of access (*e.g.*, by offering to withdraw the request in exchange for some benefit), or if the request is malicious in intent and is being used to harass the organization (*e.g.*, the request specifically states that it is intending to cause disruption). The guidance acknowledges that this is not a simple checklist and will require a detailed analysis of the request in context.

- **Controllers Can Charge a Reasonable Administration Fee When Responding to Access Requests That are Manifestly Excessive, Unfounded or Repetitive.** Controllers must not, in general, charge a fee for responding to access requests. However, when responding to requests that are manifestly excessive or unfounded (see above), or repetitive (*i.e.*, where an individual requests copies of data that has already previously been provided as part of an access request), controllers can charge a "reasonable" administration fee. The guidance sets out the factors that controllers should take into account when determining the amount of such fee, including the costs of locating and retrieving the personal data, the cost of making the personal data available to the individual (*e.g.*, over an online platform), and the amount of time spent by employees in dealing with the request. Although the guidance does not offer any suggestions on what amount would be deemed reasonable, any fee charged should reflect the actual administration costs (*e.g.*, the cost of printing, delivery charges, etc.) and, if charging for employee time, a "reasonable hourly rate," the amount of which is left to the controller's discretion.

Key Takeaways

Going forward, organizations that process EEA personal data should:

- **Train Employees and Maintain Policies To Handle Access Requests Efficiently.** This will involve, at a minimum, training employees to ensure that they are able to recognize access requests and appointing individuals to take charge of handling such requests in compliance with the GDPR time requirements. Organizations also should consider putting in place a data subject rights' request policy, including a checklist for employees, that sets out a comprehensive internal process applicable to the handling of such requests.

- **Keep a Log of All Interactions With the Individual Making the Access Request.** In compliance with the GDPR's accountability principle, organizations should ensure that they maintain a detailed record of their interactions with the requesting individual, particularly in relation to decisions to stop the clock, or where a manifestly excessive or unfounded request is denied. Individuals may choose to complain to the ICO, and such records will help organizations justify their position.

- **Avoid Habitual Reliance on the Manifestly Excessive or Unfounded Exemptions.** The inclusion of the words "manifestly" and "clearly" as part of these exemptions suggests that there is a significant hurdle to clear for such thresholds to be met. Each assessment will be dependent on context and organizations should not rely on such exemptions in the absence of compelling evidence.

Return to Table of Contents

Seventh Circuit Further Clarifies Standing in Federal Court for Illinois Biometric Privacy Act Claimants

On November 17, 2020, the U.S. District Court for the Seventh Circuit held that an Illinois plaintiff that asserted a violation of Section 15(a) of the Illinois Biometric Privacy Act (BIPA) had sufficient standing to sue in federal court in its ruling in *Fox v. Dakkota Integrated Systems*. The decision clarifies the court's May 5, 2020, decision regarding federal jurisdiction for Section 15(a) claims.

Background

The Illinois Biometric Privacy Act[3] regulates the collection, use and retention of a person's biometric identifiers or information. The BIPA imposes certain requirements on businesses that collect or otherwise obtain biometric information, including fingerprints, and retina and facial geometry scans, including obtaining the informed consent of any person whose biometric data is acquired under Section (b) of the act, and disclosing a retention schedule and guidelines for permanent destruction of collected information under Section (a) of the act.

Prior to the Seventh Circuit's ruling, there had been much discussion regarding whether certain BIPA claims could be brought in federal court, though the Seventh Circuit provided some clarity on the matter in its May 2020 ruling in *Christine*

[3] 740 ILCS 14 (2008). The text of the BIPA can be found here.

Bryant v. Compass Group USA, Inc.[4] In *Compass*, plaintiff Christine Bryant, a call-center employee, voluntarily provided her fingerprint scan to create an account with her cafeteria's vending machine that was owned and operated by Compass. Bryant alleged that Compass failed to (1) make publicly available a retention schedule and guidelines regarding the biometric identifiers and (2) obtain informed consent from the plaintiff to collect, store and use her fingerprint scan in violation of sections 15(a) and 15(b) of the BIPA. The Seventh Circuit ultimately held that, with respect to Bryant's claim under Section 15(a) of the BIPA, the duty to disclose a retention schedule and guidelines is a duty owed to the public and not one to a particular person, and therefore Bryant did not allege a particularized harm sufficient for federal standing under Article III. When the case was decided in May, *Compass* signaled that BIPA defendants may not be able to remove Section 15(a) claims to federal court.

Recent Decision

The Seventh Circuit's recent decision in *Fox v. Dakkota Integrated Systems*, however, narrows the scope of *Compass* with respect to Article III standing for Section 15(a) claims. In *Fox*, plaintiff Raven Fox was required by former employer Dakkota Integrated Systems (Dakkota) to clock in and out of work by scanning her hand on a biometric timekeeping device. Dakkota disclosed the data to third parties, including a third-party administrator that hosted employees' biometric data in a data center. Fox filed suit in state court, alleging Dakkota (1) did not obtain her informed written consent before collecting the biometric identifiers, as required under Section 15(b) of the act; (2) unlawfully provided biometric data to a third party without consent; (3) failed to develop, publicly disclose and implement a data retention schedule and guidelines for the permanent destruction of its employees' biometric identifiers, as required under Section 15(a) of the Act; and (4) failed to permanently destroy her biometric data upon her departure from Dakkota. When the defendant removed the case to federal court, the district court remanded it to the state court on the grounds that the plaintiff had insufficient Article III standing under *Compass*.

However, in *Fox*, the Seventh Circuit reversed the district court's remand order, noting in *Compass* that Bryant's Section 15(a) claim was "extremely narrow" in that it only concerned Compass's duty to publicly disclose data retention policies, which is owed to the public generally and "not to particular persons whose biometric information the entity collects." In contrast, the court held that Fox's Section 15(a) claim alleged a concrete and particularized harm arising out of more than just Dakkota's failure to publicly disclose its data retention policy. Instead, according to the court, Fox's claims alleged harms arising out of Dakkota's failure to comply with a suite of responsibilities under Section 15(a), including its duty to develop, publicly disclose and comply with its data retention and destruction policies, which resulted in the wrongful retention of Fox's biometric data after her employment ended and beyond the time authorized by law. As such, the court held that Fox's allegations were sufficient to plead an injury in fact under Article III.

The court also held that the unlawful retention of biometric data should be considered similarly with respect to the unlawful collection of biometric data, noting that, "just as [S]ection 15(b) expressly conditions lawful collection of biometric data on informed consent, [S]ection 15(a) expressly conditions lawful retention of biometric data on the continuation of the initial purpose for which the data was collected." According to the court, the BIPA's requirement to implement a data retention and destruction protocol protects a person's biometric privacy in a similar manner as the informed consent requirements under the BIPA. Therefore, the court found that the unlawful retention of a person's biometric data inflicts a privacy injury as concrete and particularized as its unlawful collection.

In its ruling, the court remanded the case to the district judge to settle issues with respect to preemption related to the Labor Management Relations Act.

Key Takeaways

The *Fox* ruling clarifies that *Compass* should be construed narrowly with respect to claims arising under Section 15(a) and that there are circumstances in which a defendant can remove Section 15(a) claims to federal court. The court's holding in *Fox* reaffirms that companies should carefully consider whether they have put proper safeguards in place to ensure BIPA compliance.[5]

Return to Table of Contents

[4] Skadden's discussion of this case can be found in the May 2020 edition of our *Privacy & Cybersecurity Update*.

[5] Certain BIPA compliance pointers may be found here.

Post-*Schrems II*: European Data Protection Board's Recommendations Clarify International Data Flows

On November 10, 2020, the European Data Protection Board (EDPB) adopted its long-awaited recommendations on (1) measures that supplement transfer tools to ensure transfers of personal data outside the European Economic Area (EEA) are adequately safeguarded (the supplementary measures recommendation) and (2) the European Essential Guarantees for surveillance measures (the surveillance recommendation). Organizations will now have a road map to follow when transferring personal data outside the EEA through a detailed multistep plan. The supplementary measures recommendation is currently in draft form and remains open to feedback through a public consultation until December 21, 2020, after which the final recommendation will be issued.

Background

Under the General Data Protection Regulation (2016/679) (GDPR), a valid data transfer mechanism must be implemented to transfer personal data out of the EEA to a country that has not been deemed by the European Commission (EC) to have an adequate level of privacy protection.

On July 16, 2020, the Court of Justice of the European Union (CJEU) ruled on two key data transfer mechanisms in *Schrems II*, invalidating the EU-U.S. Privacy Shield for data transfers to the U.S. and imposing enhanced due diligence on parties using the EC Standard Contractual Clauses (SCCs).[6] Under the ruling, in cases where such enhanced due diligence determines that the laws of the data importer's country do not provide *essentially equivalent* protection of personal data to that guaranteed under EU law, supplementary measures must be implemented. If such supplementary measures would still not provide *essentially equivalent* protection in the data importer's country, the data transfer must be suspended. The CJEU did not provide further guidance on assessing the laws of third countries, or the form that supplementary measures may take, leaving data exporters uncertain about practical next steps.

As discussed below, the EDPB's recommendations provide further clarity on these key points through a road map for organizations to follow when transferring data outside the EEA using one of the Article 46 GDPR data transfer mechanisms.

Step 1: Map and Document Your Data Transfers

The recommendations restate the obligation under the GDPR that, as a preliminary step, organizations must map, document in writing, and be accountable for their data transfers. This means that on an ongoing basis, organizations should identify (1) what data they transfer outside the EEA; (2) what countries that data is transferred to (including onward transfers); and (3) the mechanism being relied on by the data exporter to transfer the data under the GDPR. The transfer mechanism may be based on an adequacy decision, an Article 46 GPDR mechanism (such as SCCs or binding corporate rules) or an Article 49 derogation (such as where the transfer is necessary for the performance of a contract). Organizations that rely upon Article 49 GDPR derogations to transfer data outside the EEA must ensure that any such transfers are occasional and nonrepetitive, and where such transfers become regular, an alternative transfer mechanism under Article 46 GDPR should be considered.

Step 2: Do Your Diligence

Schrems II imposed the requirement that where organizations, including those located in the U.S., transfer data to a third country pursuant to an Article 46 GDPR data transfer mechanism, they need to consider whether the laws or practices in that third country would undermine the effectiveness of the selected safeguards in relation to EEA data. As described in the supplementary measures recommendation, these safeguards must "travel with the data wherever it goes." The recommendations now affirm that this will entail a thorough and documented due diligence exercise, taking into account both the third country's data privacy framework and its legal landscape more generally.

[6] For further detail on the CJEU's decision, please see Skadden's July 2020 client alert, "*Schrems II*: EU-US Privacy Shield Struck Down, but European Commission Standard Contractual Clauses Survive."

A key feature of this diligence is an analysis of the access third country public authorities will have to personal data and whether that access is limited to that which is strictly necessary. To assist with this analysis, in the surveillance recommendation the EDPB has advanced four European Essential Guarantees (EEGs) that the data exporter, with the assistance of the data importer, must assess and confirm before data can be transferred to that third country:

- **Guarantee A: "Processing should be based on clear, precise and accessible rules."** The parties should work cooperatively to identify the laws, regulatory requirements and local surveillance programs in the data importer's country that would govern the interception of individual communications. By undertaking this diligence, the parties should identify, to the extent possible, in what circumstances and on what conditions the data importer's local authorities may request or intercept personal data, whether minimum safeguards are imposed and whether the rules are actionable before a local judicial authority.
- **Guarantee B: "Necessity and proportionality with regard to the legitimate objectives pursued are demonstrated."** Organizations must consider whether the public interest objective justifies the seriousness of the interference and whether appropriate limitations counterbalance the powers of surveillance of the data importer's local authorities. Data intercepted and stored on a generalized basis will be unlikely to satisfy the requirement of necessity. The recommendations do not provide a clear road map for this analysis and the assessment of Guarantee B may be a difficult exercise for organizations to carry out in practice.
- **Guarantee C: "There should be an independent oversight mechanism."** Organizations should consider the scope of oversight afforded to the courts and regulatory authorities in the data importer's country and the extent of that oversight in practice.
- **Guarantee D: "Effective remedies need to be available to the individual."** In particular, organizations should consider whether EEA data subjects are notified when their data has been collected and whether relevant local bodies or authorities can make binding decisions on the intelligence services.

The EEGs reflect the balancing exercise that the data exporter and data importer must undertake prior to effecting a data transfer to demonstrate that a limitation on data protection and privacy rights is justifiable. However, the surveillance recommendation does not offer parties one clear, straightforward path to reach an answer to this question, and this assessment seems likely to be a challenging portion of the diligence analysis.

Step 3: Safeguard Your Transfers

As previewed in *Schrems II*, where the outcome of the foregoing diligence indicates that an essentially equivalent level of protection as granted in the EEA cannot be guaranteed in a third country, organizations must implement enhanced measures to address both: (1) the likelihood of their data being intercepted while in transit; and (2) the data importer's obligations in the context of any onward transfers (where authorized) of EEA data. On a case-by-case basis, the supplementary measures recommendation requires organizations to implement appropriate safeguards in the form of contractual and security (technical and organizational) measures to address the identified vulnerabilities in the third country prior to proceeding with the data transfer.

While the supplementary measures recommendation stresses that contractual provisions alone will not suffice, data exporters should nonetheless consider how their current contractual agreements can be enhanced by additional measures. This may include supplementary contractual requirements on the data importer to (1) implement additional technical measures (*e.g.*, encryption), (2) publish regular transparency reports detailing governmental requests to access data (*e.g.*, a table showing the number of data access requests received by the data importer on an annual basis and the percentage of those requests where data is disclosed; where the request is challenged; and where the number of records and/or data subjects disclosed is less than initially requested), (3) monitor legal and/or policy developments and inform the data exporter of any changes that may affect their continued compliance with the data transfer contractual commitments, (4) insert "*warrant canaries*," in which the data importer is required to send the data exporter cryptographically signed messages at regular intervals confirming it has not received any disclosure requests that would involve EEA personal data, and (5) assist with the handling of EEA data subject rights requests. Depending on the outcome of the diligence exercise, the supplementary measures recommendation encourages organizations to implement these measures as soon as reasonably practicable. Contractual provisions can be implemented immediately and, unless they conflict with the SCCs, do not require preapproval from the competent supervisory authority.

Many of these contractual safeguards have been incorporated into the new draft SCCs, published by the EC on November 12, 2020, and currently under public consultation until December 10, 2020 (There will be a one-year grace period applicable to the new set of SCCs). When implementing supplemental contractual protections with the data importer, the data exporter may wish to incorporate or make reference to these new draft SCCs.

The supplementary measures recommendation also advises data exporters to consider the following technical and organizational measures:

Supplementary Measures Recommendation	
Technical Measures	– Encryption with algorithms that are "flawlessly implemented" (*e.g.*, by software certified to be specified to that algorithm). – Control over decryption, in transit and at rest, retained by data exporters located in the EEA or a country subject to an adequacy decision. – Pseudonymization, where the data exporter alone retains control over reidentification. – Split or multiparty processing (with sensitivity to any collaboration between public authorities).
Organizational Measures	– Internal policies of the data importer that allocate responsibility amongst employees for data transfers and implement procedures relating to the receipt and escalation of public authority requests for access to personal data. – Training for employees of the data importer to manage public authority requests for access to personal data. – Implementation by the data importer of strict data access controls (on a need-to know-basis) on receipt of data and appropriate internal confidentiality policies.

Careful attention must be paid to the supplementary measures recommendation's conclusion that no technical measures exist that could sufficiently safeguard the data transfer where (1) that data is transferred to processors in third countries who require access to that data "in the clear," or unencrypted, to execute their assigned task (*e.g.*, cloud service providers) or (2) remote access to data is given to data importers in third countries for shared business purposes (*e.g.*, intra-group data transfers). In these instances, organizations should consider whether an Article 49 derogation may apply (such as an instance where a transfer is necessary for the performance of a contract) or suspend such transfers. The exact scope of the supplementary measures recommendation's position on these two transfers is not clear and ideally further clarity will emerge following the consultation period.

Looking Ahead

The recommendations set forth the mandatory approach that organizations in all countries must follow when transferring EEA data to countries that have not received an adequacy decision. Currently, only Andorra, Argentina, Canada, the Faroe Islands, Guernsey, Israel, the Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay have been recognized by the EC as providing adequate protection, and these adequacy decisions are under continued review.

In the absence of an EC adequacy decision in favor of the U.K. post-Brexit, transfers of data from the EEA to the U.K. will require diligence of the U.K.'s data protection legislation and legal landscape more generally.

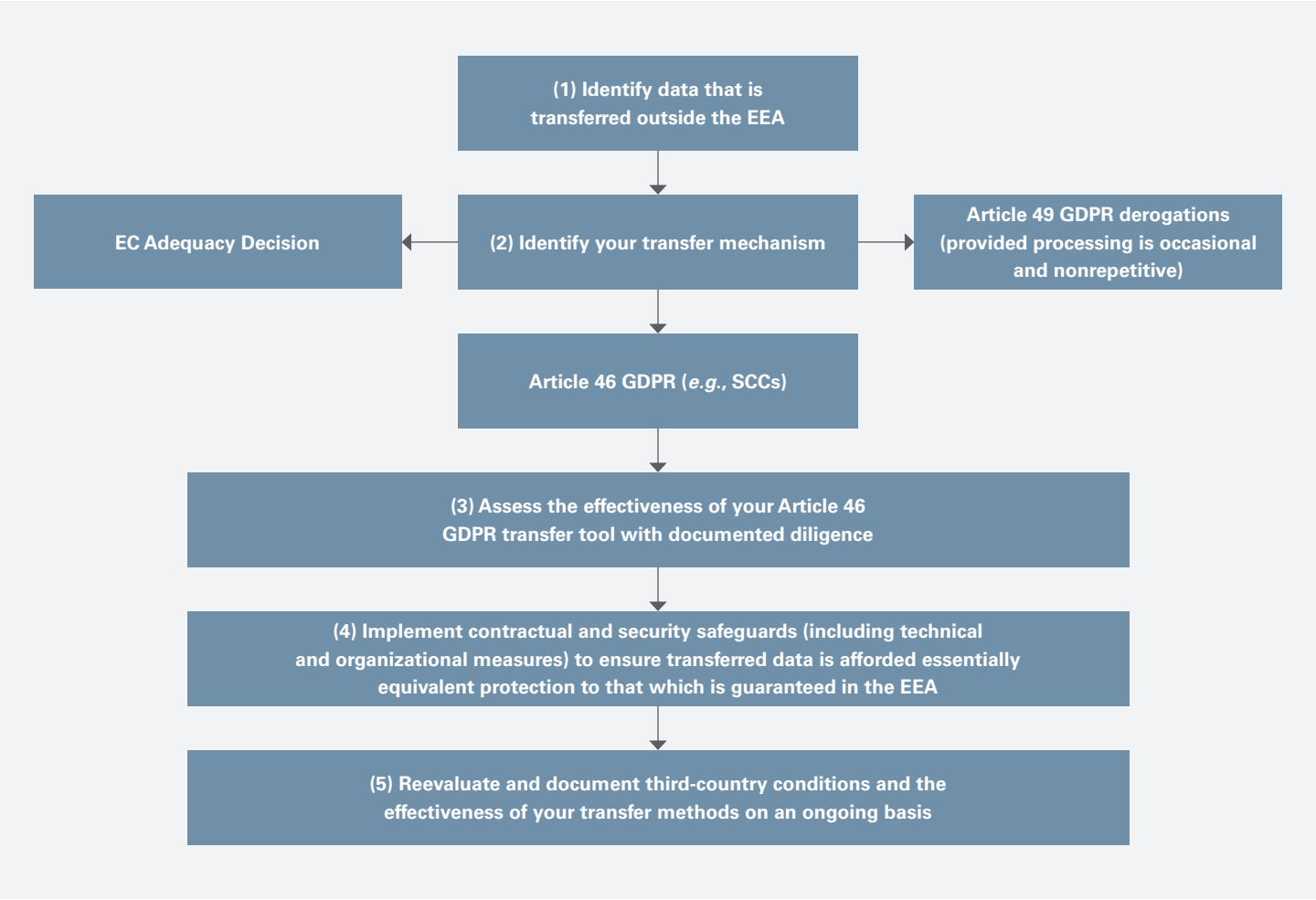
In the U.S., it is too early to tell whether President-elect Joe Biden's administration will take a different approach to privacy issues, particularly given the inherent tension that the *Schrems II* decision creates between privacy rights and the activities of law enforcement and intelligence agencies.

Key Takeaways

- As set forth in the flow chart below, the recommendations provide a welcome transfer toolkit and step-by-step guidance that organizations both inside and outside the EEA should refer to throughout the life cycle of their data transfers to third countries. Going forward, the positions taken in the recommendations that currently lack sufficient clarity ideally will be refined through the consultation process. Organizations should start reviewing their data maps and transfers, both current and proposed, and, where appropriate, implement the relevant set of supplementary measures or consider, where no suitable alternatives are available, seeking the competent EEA supervisory authority's authorization and/or, if none of these options is viable, temporarily suspending any transfers which would be deemed noncompliant.

- It also is crucial that organizations now carry out transfer impact assessments (prior to transfer), regularly monitor their data transfers and document all actions, including diligence, and decisions relating to such transfers. The duty to be "on top of your transfers" will include continued reassessment of the laws of the third countries to which data is transferred and the corresponding adequacy of the adopted data transfer mechanism.

Step-by-Step Data Transfer Process Under the EDPB's Recommendations



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
213.687.5010
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

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