JANUARY 26, 2022

2022 - Year of the Privacy Contract Update: Why Changes on Both Sides of the Pond Make Now the Time to Start Updating Your Privacy Contracts

Most New Year's resolutions can fall by the wayside, but there is one you will need to keep in 2022 – updating your privacy contracts. This year, privacy professionals will need to spend a significant amount of time updating privacy-related contracts to comply with developments in both Europe and the United States. Otherwise, you'll have your contractual counterparties, or even worse, data protection authorities or attorney generals knocking on your company's front door.

I. Europe: Updating Contracts with EU and UK Standard Contractual Clauses; New Compliance Hurdles for Processors

For organizations subject to the European Union's General Data Protection Regulation ("GDPR"), it's imperative to update your Data Processing Agreements ("DPAs") in 2022 if you rely on standard contractual clauses ("SCCs") for the transfer of personal data outside of the European Economic Area ("EEA"). On June 4, 2021, the European Commission adopted SCCs that businesses may use as a tool to comply with European cross-border data transfer requirements for transferring data outside of the EEA. Parties currently using the prior version of the SCCs had until September 27, 2021 to start using the new SCCs for all new data arrangements and will have until December 27, 2022 to replace the prior SCCs currently in effect. If the underlying agreement between the parties is re-negotiated or the scope of the data being processed changes during the transition period, the parties must use the new SCCs.

Given the *Schrems II* decision and additional scrutiny on data transfers to the United States, organizations will need to review what supplementary measures are in place, and conduct any necessary transfer impact analyses.

With respect to the United Kingdom, the Information Commissioner's Office has not yet finalized its version of the SCCs, but additional guidance is expected in early 2022. Once these SCCs are finalized, companies that process personal data from the United Kingdom will need to incorporate them into their 2022 privacy contract updates.

Vendors that act as processors often contractually carve out additional use rights in personal data that the processor chiefly uses on the controller customer's behalf. Guidance released in January 2022 by the CNIL, the French data protection authority, makes reserving such use rights considerably more difficult for vendor processors. According to the CNIL, the controller customer must approve, in advance and in writing, any processing carried out for the processor's own purposes. A general authorization in the DPA is insufficient. As such, processors should update form DPAs to provide a streamlined mechanism through which their controller customers may provide written authorization for new processing purposes. The CNIL also noted that the initial controller must inform data subjects of the processing (parties often attempt to meet this obligation by requiring the "customer" controller with privity to the data subjects to

display or link to the vendor's privacy notice). Note, however, that the controller is allowed to delegate to the processor the obligation to provide notice to the data subjects if the processor has the contact information of the data subjects. Finally, although not necessarily a change from parties' previous understanding of obligations, the CNIL emphasized that the initial processor would act as a controller with respect to any processing for its own purposes and be subject to the full scope of GDPR obligations for controllers.

For a more detailed discussion about negotiating the scope of vendors' use rights in DPAs, please review this article.

II. United States: Updating Contracts for Upcoming State Laws

a. California

The California Privacy Rights Act of 2020 ("CPRA"), which amended the existing California Consumer Privacy Act ("CCPA"), will become effective on January 1, 2023. Your updates for the CPRA will likely need to wait until the newly-formed California Privacy Protection Agency finalizes the associated regulations later this year (hopefully in July 2022). For example, the forthcoming CPRA regulations are expected to further clarify for what purposes service providers may use and combine personal information otherwise processed on a business customer's behalf.

There are, however, updates to consider since it is possible (if not highly likely) that the California legislature will not act in time to prevent the sunset of the employee data exemption from the CPRA. If employee data becomes subject to the CPRA on January 1, 2023, it is critically important to ensure that all vendors who receive the personal information of job applicants, employees, independent contractors and other personnel are contractually obligated to limit the vendors' rights to use and sell such personal information (i.e., ensuring that the vendors act as "service providers" under the CCPA). Please continue to monitor this issue closely.

b. Virginia

Similar to the CPRA, the Virginia Consumer Data Protection Act ("CDPA") takes effect on January 1, 2023. If an organization is subject to the CDPA, the CDPA requires a controller and processer to have a DPA in place. Under the CDPA, the DPA must clearly set forth: 1) the instructions for processing data, 2) the nature and purpose of processing, 3) the type of data subject to processing, 4) the duration of processing, and 5) the rights and obligations of both parties. The CDPA imposes a number of contractual requirements for processors, including that the processor must: 1) ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data, 2) at the controller's discretion, delete or return all personal data, unless retention is required by law, 3) upon reasonable request of the controller, make available information demonstrating compliance with the CDPA, 4) allow, and cooperate with, reasonable assessments by the controller or conduct an independent assessment of the processor's policies and technical and organizational measures, and 5) engage a subcontractor pursuant to a written contract that requires the subcontractor to meet the obligations of the processor with respect to personal data. As many of the CDPA's DPA requirements are similar to the GDPR, organizations subject to the GDPR will likely have light updates to make to their DPAs (but should check that the DPA applies to the personal data of data subjects outside of Europe). On the other hand, organizations that have not already prepared for the GDPR may have to undertake significant edits.

c. Colorado

Lastly, the Colorado Privacy Act ("CPA") will take effect on July 1, 2023 and also requires the controller

and processor to enter into a DPA. The CPA imposes similar contracting requirements to those of the CDPA. However, the CPA also explicitly states that in no event may a contract relieve a controller or processor from liabilities imposed by virtue of the processing relationship. Also, like the GDPR (but unlike the CDPA), the CPA requires that the controller have the opportunity to object to the engagement of a sub-processor.

III. Attacking the Challenge

To fully take the tiger by the tail this year in facing the challenge of updating potentially hundreds or thousands of contracts, it is important to be organized and get an early start. Many organizations have prepared DPA playbooks and trained employees (e.g., procurements teams), outside contractors or attorneys on how to negotiate DPAs on their behalf. Also, one benefit to starting early on this project is to send out your organization's form DPA first before you hear from your counterparties. Starting with your preferred form will result in a more favorable negotiating position and help you end up with signed DPAs that make sense for your company.

Given the size of the task ahead, it's best to start as soon as possible. Hopefully the updates you make this year will lay a solid foundation for any state or global privacy laws that may pass in 2022 (assuming Europe doesn't issue new SCCs or prohibit data transfers altogether).