DECEMBER 15, 2022

Countdown to 2023: Privacy Compliance Checklist for The End of The Year

by Jon Neiditz , Vita E. Zeltser

In January of 2022, we recommended adding "updating privacy contracts" to your list of New Year's resolutions. With 2023 around the corner and a number of new privacy laws and regulations going into effect, we have another list for you. This time, we'll call them "Pre - New Year's Resolutions" because you'll want to have some of these to-dos done (or at least started) before January 1st. Ideally, this will serve as a year-end review checklist, because most of you have been keeping up on these issues with us all year (or longer)!

I. Set Your Websites to Respond to Global Privacy Control Signals

Going back to July 2021, we warned that California regulators focus CCPA enforcement on how businesses respond to opt out of sale (and soon share) requests. As part of that response, according to the California regulators, is honoring GPC signals as a valid opt out (at least with respect to the browser or device that sends the signal).

Recent developments indicate that almost all businesses should respond to GPC signals. First, California's draft regulations limit how service providers may use personal information, meaning that more ad tech vendors cannot act as service provider (increasing the number of potential "sales"). Second, the new privacy agency in California appears to have side stepped statutory updates that make the GPC response optional, instead requiring businesses to respond to the signal in the draft regulations. Third, a recent enforcement action against Sephora (we describe it here) highlighted that the California Attorney General considers that any web tracking not done on a service provider basis (which cannot include tracking for targeted advertising) to be a "sale" under the CCPA that must be disabled in response to a GPC signal.

California regulators' positions may be challenged through litigation. For example, litigants might allege that the CCPA's definition of "sale" is void for vagueness, requiring the GPC response is *intra vires* regulation, and/or that the CCPA violates the dormant commerce clause. Until such a challenge, however, companies should avoid regulatory scrutiny by responding to GPC signals.

II. On January 1, the CCPA Applies to Employees, Applicants and Business Partners

As we warned you in June, the CCPA's general provisions, as amended by the California Privacy Rights Act (CPRA), will now apply not only to your California consumers but to your employees, applicants, contractors and business partners who are California residents. We emphasized how unintended and devoid of privacy benefits this fruit of legislative inertia would be, and the regulators appear to agree, so it is unclear whether this will likely be an area of vigorous enforcement. Nonetheless, to comply with CCPA, your company should meet the following three requirements by year-end:

1. Employee Notice – When the CCPA first became effective, you sent out limited notices to your

California employees and job applicants. Now you need to issue a more fulsome notice to them, explaining not only the types of personal information collected and the purposes for which that information will be used, but also CCPA rights (which are subject to significant exceptions--see below) and disclosures about how you share their information. One way to prepare this notice is by basing it on the privacy notice you have posted for consumers, and tailoring it for employees and the specific information that will be collected from them.

2. Employee Requests to Exercise Rights – Technically, your employees, applicants, contractors, and business partners can now exercise "consumer rights under the CCPA (e.g., the right of access, correction and deletion).So you do need to establish a procedure that allows employees to exercise these rights and another that allows for verification and response to employee requests in connection with these rights. HR staff will likely need to be trained on how to handle and respond to these requests (including that all such requests should undergo legal review given that such requests will be used to preempt discovery in employment litigation). Remember, though, as we said in June, that these requests are likely to focus on access, and deletion may often not be permissible, and also consider how to implement the draft rules new and now more specific "disproportionate effort" standard.
3. Agreements with Vendors – Take a second look at your contracts with any vendors that handle employee, applicant, contractor and business partner information. These contracts should include specific clauses mandated by the CPRA, including the prohibition of any onwards sale or sharing of personal information.

We wrote earlier this year about a likely increase in CCPA enforcement by the California Attorney General, and this prediction held and continues to hold true . Enforcement of the new CPRA provisions is set to begin in July of 2023. This gives companies a short period of time to come into compliance; as suggested above, we recommend focusing particularly on the consumer side. Remember, the 30 day notice and correction period becomes optional next year, so regulators need not permit companies to come into compliance before bringing an enforcement action.

Four New State Laws Becoming Effective in 2023

In addition to the CPRA, there are four new state laws going into effect in 2023. If you haven't done so already, we recommend examining whether these laws apply to your organization before January 1, 2023 to ensure timely compliance. Fortunately all of these laws exclude employee and B2B personal data from their scope. To see if these laws (and California's) may apply to your organization, please take our privacy legislation applicability questionnaire. You can also use the information below as a quick reference guide to see which, if any, of these state laws may apply to your organization. Links are also provided to our in-depth analysis of each law.

Virginia Consumer Data Protection Act (VCDPA) – Effective January 1, 2023 – The VCDPA applies to businesses in Virginia or businesses that produce products or services targeted to residents of Virginia, and that:

a. During a calendar year, control or process the personal data of at least 100,000 Virginia

residents, or

b. Control or process personal data of at least 25,000 Virginia residents and derive over 50% of gross revenue from the sale of personal data.

Colorado Privacy Act (CPA) – Effective July 1, 2023 – The CPA applies to companies – including, uniquely, nonprofits – that conduct business in Colorado or produce or deliver commercial products or services targeted to residents of Colorado and satisfy one of the following thresholds:

a. Control or process the personal data of 100,000 or more Colorado residents during a calendar year; or
b. Control or process the personal data of at least 25,000 Colorado residents and receive revenue or a discount on the price of goods or services from the sale of personal data.

If the CPA applies to your organization, please be sure to take a look at the draft rules.

Connecticut Data Protection Act (CTDPA) – Effective July 1, 2023 – Connecticut's law applies to any company that conducts business in the state or has goods or services that target residents of the state, and:

a. Controls or processes personal data of 100,000 or more Connecticut residents; or
b. Controls or processes personal data of at least 25,000 Connecticut residents and derives over 25% of gross revenue from the sale of personal data.

Utah Consumer Privacy Act (UCPA) – Effective December 31, 2023 – This law applies to any company that conducts business in the state or targets residents of the state, has an annual revenue of $25 million or more, and:

a. Controls or processes personal data of 100,000 or more Utah residents; or
b. Controls or processes personal data of at least 25,000 Utah residents and derives over 50% of gross revenue from the sale of personal data.

There are steps you can take to ensure compliance with most or all of these new laws simultaneously, including updating privacy policies, reviewing agreements with vendors with whom you share personal information, implementing procedures to receive, verify, and respond to requests from consumers, reviewing your cyber security protections, and training employees. Critically, several of these forthcoming state laws are more strict in that they require opt-in consent for processing sensitive personal data (i.e., information like ethnicity, precise geolocation, and religion that your marketing departments might be currently using).

III. Keep an Eye on the EU

Given all of the DPAs that you've likely negotiated this year before the December 27, 2022 deadline, you probably don't want to think about EU – US data transfers, but there has been an important development. After months of negotiations, the U.S. and EU announced in March 2022 that they had reached an agreement on a proposed replacement for the EU-U.S. Privacy Shield, entitled the EU-U.S.

Transatlantic Data Privacy Framework. In October, 2022, the U.S. government issued executive actions in support of its commitments to the Transatlantic Data Privacy Framework. A new Executive Order ("EO"), issued by the White House, and accompanying regulations, issued by the U.S. Department of Justice ("DOJ"), are intended to address the concerns of the *Schrems II* court regarding the protection of EU personal data against government access and the lack of a sufficient redress mechanism for individuals to challenge such decisions. The EO is the latest and most significant step towards finalizing the EU-U.S. Transatlantic Data Privacy Framework.

The EO and DOJ regulations are intended to expand protections for EU persons with respect to surveillance, and to limit surveillance to what is "necessary and proportionate." The regulations will also establish a new redress mechanism to address challenges to the collection of personal data, including an initial review by a Civil Liberties Protection Officer ("CLPO") (essentially a DPO for the U.S. intelligence community), and a second level of binding review by the Data Protection Review Court ("DPRC"), an Article II court which will be comprised individuals independent of the government. In addition, U.S. intelligence services are to update policies and procedures on an ongoing basis, and the Privacy and Civil Liberties Oversight Board ("PCLOB") is to review those policies as well as conduct an annual review of the redress mechanism. On December 13, 2022, the EC announced its adequacy decision, based on the EO and DOJ regulations, which implement the March framework agreement into U.S. law. The draft adequacy decision sets in motion the adoption procedure of review and/or approval by other EU entities, e.g., the European Data Protection Board ("EDPB"), which will review the draft next, the European Parliament ("EP"), Council of Europe, and approval by Member States. This development signals very strong support for the new framework and the robustness of the new EO and DOJ regulations. The EC announced that the decision "reflects the assessment by the Commission of the US legal framework and concludes that it provides comparable safeguards to those of the EU."

Although the approval process will take some time, organizations may go into the new year with a glimmer of optimism to share with EU partners; according to the EC, "European companies will be able to rely on these safeguards for trans-Atlantic data transfers, also when using other transfer mechanisms, such as standard contractual clauses and binding corporate rules." For transfers to companies that eventually participate in the framework and adhere to its obligations, EU entities will no longer have to put "additional safeguards" in place, a welcome development to combat the post-holiday winter blues. While we eagerly await the finalization of the new data transfer framework, there are a few steps companies can take now to keep transfers running smoothly:

- Evaluate, document, and if necessary, implement additional safeguards for cross-border data transfers;
- If your company exports personal data from the EU/UK, conduct transfer impact assessments (TIAs) to ensure compliance with the GDPR; and
- Continue to monitor developments out of the EU.