MILLER CANFIELD

Recent Developments in Data Privacy Laws Impacting U.S. Companies

November 18, 2020

American companies should take notice of some important developments in data privacy laws in the U.S. and in the European Union.

California Privacy Rights Act

On November 3, 2020, California voters approved the California Privacy Rights Act ("CPRA," a.k.a. "Proposition 24" or "CCPA 2.0"). The CPRA, which amends and expands the existing California Consumer Privacy Act of 2018, will become effective as of January 1, 2023, and enforceable on July 1, 2023.

Most significantly, except for access request, which from January 1, 2022 will not be limited to a 12-month window, the CPRA imposes new obligations relating to any personal information a business collects on or after January 1, 2022, including expanding the opt-out right to "sharing data," granting right to correct inaccurate information, or introducing data mineralization and purpose limitation obligation. The CPRA also modifies the applicability threshold, extends the B2B and employee exemption, identifies "*sensitive*" personal information and expands protection thereof, provides transparency around automated decision making, and establishes the California Privacy Protection Agency as the governmental agency charged with enforcement.

Data Transfer from the E.U. to the U.S.

On July 16, 2020, the Court of Justice of the European Union in the "*Schrems II*" decision invalidated the Privacy Shield Framework that many entities relied on when transferring personal data from the E.U. to the U.S. At the same time, while upholding the validity of contractual clauses, which constitute one of the transfer mechanisms under the E.U.'s General Data Protection Regulation ("GDPR"), the court held that contractual clauses are solely intended to provide contractual guarantees among parties, and cannot bind public authorities of third countries. Therefore, when personal data is transferred to a country that does not legally ensure adequate data protection, the "controller" (the entity that determines the purposes and the means of processing personal data) may be required to adopt supplementary measures. Where the controller or a processor (the entity that processes personal data on behalf of the controller) is not able to adopt adequate additional measures or fails to implement them, the data transfer should be suspended and the contract terminated by the parties. Otherwise, the competent supervisory authority must suspend or end the data transfer.

The court did not specify the character of such supplementary measures. This issue was addressed in Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (draft), adopted by the European Data Protection Board on November 10, 2020. Based on the principle of accountability and the right to data protection recognized by European law, the Recommendations have introduced a roadmap of steps that will help determine if the data exporter should put supplementary measures in place. These steps include being aware of what kind of data transfer is at stake, identifying the transfer tools relied on, assessing if the transfer tools are effective in the light of the circumstances of the transfer, and finally, where the analysis concludes that the employed measures are not effective, what supplementary measures should be adopted, and later, re-evaluated at appropriate intervals. The Recommendations list examples of such measures, dividing them into three categories: technical, contractual and organizational.

Continued

Most recently, on November 12, 2020, the European Commission published a first draft of new contractual clauses applicable to data transfers to a non-EU processor, sub-processor or controller, including transfers made by a non-EU processor or a controller with respect to data governed by the GDPR. The clauses contain several modules, depending on the type of transfer and the parties involved. According to the *Schrems II* decision and the European Data Protection Board Recommendations, the clauses also provide for specific safeguards that address the effects that the law of the country of destination may have on the data importer's compliance with the clauses, as well as how such a data importer should deal with binding requests from public authorities for disclosing the personal data transferred. The draft provides for a grace period of one year for data exporters and importers to implement the new clauses.

We expect further developments in all above areas, so look for additional information from Miller Canfield. Please contact the authors or your Miller Canfield attorney to discuss further.