CLIENT ALERTS & INSIGHTS

Privacy Points 2023: Contractual Provisions Required as New State Laws Regulate the Sharing and Processing of Personal Information by Third Parties

FEBRUARY 23, 2023

The ability to verify compliance with applicable law, notice and opt-out requirements for subcontractors, and flowing through data minimization principles are key requirements under new US state data protection laws.

As the new US state data protection laws are taking effect at the beginning of 2023 and continuing throughout the rest of the year, businesses have focused on what internal mechanisms, policies, and procedures-such as internal assessments and policies related to sensitive personal data-must be in place to comply with the new privacy and information security requirements.

Beyond controls and measures placed on businesses, each new US state data protection law also requires in-scope businesses to consider certain data privacy and information security principles in it contracts with third parties that will have access to or otherwise process personal information on the business's behalf.

The flow-through contractual requirements generally work to further four principles: (1) data minimization principles-using the minimum amount of information, for specified purposes and periods of time; (2) data subject privacy rights; (3) appropriate and reasonable security measures; and (4) ensuring adherence to applicable data protection laws. Some examples of more stringent requirements include requiring an opportunity to new subcontractors who will be processing or accessing the personal information and providing assistance in complying with data subject rights requests (e.g., deleting personal information).

Below are descriptions of the new contractual requirements that are set forth under the respective U.S. data protection laws that are either in affect already or coming into effect over the course of 2023.

California Service Providers and Contractors

California's data protection regime-which is effective as of Jan. 1, 2023 and enforceable this coming summer-sets forth three categories of third parties who have access to or process personal information: (1) Service Providers; (2) Contractors; and (3) Third Parties.

Service Providers are those parties who process and use the personal information on behalf of the in-scope business; while Contractor are those parties who have access to personal information originally collected by the in-scope business. If a third party qualifies as a Service Provider or as a Contractor, the personal information sharing and relationship is **not**

considered a sale under the CCPA. This is important as "sales" under the CCPA trigger additional requirements and obligations on in-scope businesses, including the right for individuals to opt-out of any such sale.

If a party simply qualifies as a Third Party, the relationship is not exempt from the "sale" obligations under the CCPA. However, it is important to note that all three relationships and categories of third parties are subject to contractual requirements.

Service Provider and Contractor Requirements

First, to qualify as either a Service Provider or Contractor, the third party must agree via a contract to only use the personal information for limited purposes.

Specifically, the Service Provider or Contractor can only use or process personal information (1) the specified business purposes as set forth in the contract, mutually agreed to between the parties; (2) to retain subcontractors; (3) to prevent, detect, or investigate security incidents or protect against viruses and malware; and (4) for internal use by the service provider or contractor, but only to build or improve the quality of the services it provides to the specific business. The fourth possible use of personal information is only allowed where the Service Provider or Contractor does not use the personal information to perform services on behalf of another business or party.

It is important to note that a third party who provides cross contextual behavioral advertising cannot be considered a Service Provider under applicable California regulation. Cross-contextual behavioral advertising includes the targeting of advertising to a individual based on the individual's personal information obtained from their activity across businesses, distinctly- branded websites, applications, or services, other than the specific in-scope business's, distinctly-branded website, application, or service with which the individual intentionally interacted with.

Second, the Service Provider or Contractor must agree to specific obligations and measures via a written contract.

In order for a third party to be considered a Service Provider or Contractor under the CCPA there must be a contract in place that (1) prohibits them from selling or sharing the information; (2) identifies the specific business purposes for the Service Provider or Contractor is processing the information (in specific terms); (3) prohibit the retention, use, or disclosure of the information for any purposes beyond those specified business purposes; (4) prohibit the processing of the information outside of the direct business relationship between the Service Provider or Contractor and the business; (5) require compliance with the CCPA-including, without limitation, the information security requirements; (6) allow the business to take "reasonable and appropriate steps" to ensure the Service Provider or Contractor is compliant with the CCPA and the contract; (7) require notification to the business where the Service Provider or Contractor determines it is unable to comply with the CCPA; (8) allow the business to take reasonable steps to stop and remediate any unauthorized use of the information; and (9) require the Service Provider or Contractor to enable the business to comply with applicable individual data privacy right requests or to inform the business where such requests are made.

On the last point, from a practical perspective, in-scope businesses will need to ensure to some degree of certainty that the Service Providers or Contractors are complying with reasonable

instructions pursuant to an applicable data subject right request. Failing to do so risks liability for failure to comply with data subject requests.

Third Party Requirements

Even if a party does not fall under the Service Provider or Contractor distinctions, a written contract is required by the CCPA. The requirements are less onerous on the third party, however, because the relationship would be considered a "sale" there are more onerous obligations placed on the in-scope business as discussed above.

Third Party contracts must (1) identify the limited and specific purposes for which the information is sold or shared with the third party; (2) specify the business is selling or sharing the information for the limited and specific purposes identified in the first requirement; (3) require compliance with the CCPA-including, without limitation, the information security requirements; (4) allow the business to take "reasonable and appropriate steps" to ensure the third party is compliant with the CCPA and the contract; (5) allow the business to take reasonable steps to stop and remediate any unauthorized use of the information; and (6) require notification to the business where the Third Party determines it is unable to comply with the CCPA.

An additional point to consider is data subject right requests. Even though the relationship is with a Third Party, setting up a notification and compliance procedure and mechanism for data subject right requests is something parties will need to consider to comply with the CCPA.

Colorado, Virginia, and Connecticut Processors

Colorado's, Virginia's, and Connecticut's new data protection regimes set forth a simpler third party dynamic. Under these new U.S. state data protection laws, parties are either considered a "controller" or a "processor". A party is a controller if they-alone or in joint decisions with others-determine the purposes for and means of processing personal information. A party is a processor if they are processing the personal information on behalf of the controller.

Like California, a contract is required in all cases when personal information is shared or accessible to a third party.

To effectuate a controller - processor relationship, the controller and processor must enter into a binding contract that delineates the parties' respective responsibilities and the processing instructions the processor must adhere to. The contract between the two parties must contemplate and provide that (1) each person involved in processing is subject to a duty of confidentiality with respect to the personal data; (2) at the controllers direction and option, for the processor to delete or return personal data to the controller (unless prohibited by applicable law); (3) audit and review obligations that allow the controller to ensure the processor is complying with the applicable law; and (4) only engage subcontractors pursuant to written contracts that set forth the same or heightened obligations on the subcontractor; and (5) only disclose the information to subcontractors after giving the controller a reasonable opportunity to object to the engagement of such subcontractor.

Practically-and in line with the requirements set forth in California-controllers will likely need to set up express requirements around notifications for and compliance with data subject right requests.

Utah Processors

Utah sets up the same categories of parties as Colorado, Connecticut, and Virginia: controllers and processors.

Under Utah's more business-friendly law, fewer requirements are needed than under the similarly structured Colorado, Virginia, and Connecticut laws. The controller-processor contract under Utah law must: (1) clearly set forth the instructions for processing the applicable information, the nature and purpose of the processing, type of information in scope, and the duration of the processing; (2) require each person involved in processing to be subject to a duty of confidentiality with respect to the information; and (3) only allow the engagement of subcontractors pursuant to written contracts that set forth the same or heightened obligations on the subcontractor.

Still though, Utah's data protection law provides individuals with certain privacy rights. In line with the other states, controllers will likely need to set up express requirements around notifications for and compliance with data subject right requests.

Moving Forward: Contracts Are Key

No matter the relationship between a business subject to new U.S. state data protection and their third party providers, a written contract that contemplates specific requirements with regard to data security and privacy will be required.

But beyond hard-and-fast legal requirements, practical considerations like data subject right request notification and compliance are key to proper written agreements contemplating sharing or accessing personal information.

As more states continue to implement their own variations of data protection laws and business juggle the various requirements, the Benesch Data Protection and Privacy team is committed to staying at the forefront of knowledge and experience to assist our clients in compliance efforts. We are available to assist you with any compliance needs.

Lucas Schaetzel at lschaetzel@beneschlaw.com or 312.212.4977.