Kilpatrick

September 5, 2023

Vendor Management from a U.S. Data Privacy Perspective

by John M. Brigagliano

Given the increasing number of data privacy laws in the U.S., entering into appropriate data processing agreements ("DPAs") with vendors has now become a critical component of vendor management. It can also be one of the most time-consuming and complex aspects of data privacy compliance. This article discusses when an organization should enter into a DPA with a vendor, an overview of U.S. DPA requirements, key considerations when negotiating a DPA, and some other key aspects of vendor management from a U.S. data privacy perspective besides entering into a DPA.

When an Organization Should Enter into a DPA with a Vendor

At the onset of the vendor relationship, it is critical to determine whether a DPA is legally required. Current or forthcoming comprehensive data privacy laws in certain U.S. states[1] contain various contractual requirements, which is a driving factor in the rising number of DPAs in the U.S.

As a first step in determining whether to enter into a DPA, it is important to understand whether either or both the organization (or customer) and the vendor are subject to the U.S. comprehensive data privacy laws that would mandate a DPA. Although thresholds vary by state, generally U.S. state comprehensive data privacy laws have high thresholds for applicability (e.g., $25 million in gross annual revenue, processing the personal data of 100,000 consumers in a given state, or significantly engaging in the "sale" of personal data), which means that they do not apply to many smaller organizations. If both the customer and the vendor are not subject to these laws, then no DPA is legally required. However, a customer may still want to negotiate a DPA to afford adequate contractual protections for the personal data provided to the vendor.

Next, if either the customer or the vendor is subject to these laws, DPAs are only legally required where "personal data" or "personal information" (i.e., information that is linked or reasonably linkable to an identified or identifiable individual) is being disclosed to the vendor. Therefore, if the information being disclosed to the vendor does not constitute personal data under applicable law or if the information has been sufficiently de-identified or aggregated so that it is no longer personal data, a DPA is not legally required.

As contractual requirements under U.S. state comprehensive data privacy laws generally only apply when the vendor is acting as a "processor" (i.e., processing the personal data on behalf of the customer) or a "service provider" (i.e., using the personal data only for a specified business purpose), it is important to look at each vendor critically to determine its role. If the vendor is not providing a traditional service offering such that the vendor is not processing the personal data on the customer's behalf or using the personal data outside of the

specified business purpose, then no DPA may be legally required and/or a modified DPA might be preferred. Examples of such vendors include integration partners and data brokers.

Lastly, other state laws and federal laws may impose contractual requirements for certain types of data or for certain industries, which also might be exempt from the comprehensive data privacy laws. For example, recently enacted laws governing "consumer health data" in Nevada[2] and Washington[3] contain detailed contractual requirements (such as requiring a vendor to act consistently with the customer's consumer health data privacy policy). On a federal level, the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule contain detailed contract requirements for in-scope service arrangements. U.S. financial privacy laws also may shape DPAs, as financial institutions must monitor and assess their vendors' data security capabilities.[4]

Overview of U.S. DPA Requirements

For those instances where a vendor is processing personal data on the customer's behalf, the following are contractual requirements common across the various U.S. state comprehensive data privacy laws:

- The customer's instructions for the vendor's processing of the personal data, including the nature and purpose of processing;
- Identifying the type of personal data to be processed by the vendor;
- Identifying the rights and obligations of the customer and the vendor;
- Outlining the duration of the vendor's processing;
- Ensuring that the vendor requires each individual processing the personal data to be subject to a duty of confidentiality with respect to the personal data;
- Requiring the vendor to only engage subcontractors that meet the same obligations of the vendor with respect to the personal data being processed, and, in certain states, requiring the vendor to obtain written permission from the customer before engaging a subcontractor;
- The vendor making available to the customer upon request any information necessary to demonstrate its compliance under the DPA and applicable law;
- Requiring the vendor to cooperate with reasonable assessments and audits, either by the customer or a third-party auditor; and
- At customer's direction, requiring the vendor to delete or return all personal data to the customer after the provision of the service is completed, unless retention of the personal data is required by law.

In addition to the above, the California Consumer Privacy Act, as amended by the California Privacy Rights Act (collectively, the "CCPA") imposes unique contractual requirements. The CCPA requires businesses to use mandatory language in their contracts with vendors that complies with the following obligations:

- Prohibiting the vendor from "selling" or "sharing" the personal data;
- Specifying the business purpose for which the vendor is processing the personal data for the customer;
- Prohibiting the vendor from retaining, using, or disclosing personal data for any purpose other than the specified business purpose or outside of the direct business relationship between the vendor and the

customer, unless expressly permitted by the CCPA;

- Requiring the vendor to comply with all applicable sections of the CCPA, including providing the same level of privacy protection as required by the customer under the CCPA, which may include cooperating to respond to consumer requests under the CCPA;
- Granting the customer the right to take reasonable and appropriate steps to ensure that the vendor uses the personal data in a manner consistent with customer's obligations under the CCPA, which may include, for example, ongoing manual reviews and automated scans of the vendor's systems and regular internal or third-party assessments, audits, or other technical and operational testing;
- Requiring the vendor to notify the customer after it makes a determination that it can no longer meet its obligations under the CCPA;
- Granting the customer the right, upon notice, to take reasonable and appropriate steps to stop and remediate the vendor's unauthorized use of personal data. Reasonable and appropriate steps may include, for example, requiring the vendor to provide documentation that verifies that the vendor no longer retains or uses personal data of consumers that have made a valid deletion request; and
- Requiring the vendor to enable the customer to comply with consumer requests under the CCPA or require the customer to inform the vendor of any consumer requests under the CCPA and provide information necessary for the vendor to comply with such requests.

The CCPA is also unique in that even if a vendor does not process the personal data on the customer's behalf (such that the customer is "selling" personal data to the vendor), certain contractual requirements still apply. Such requirements include provisions limiting the vendor's use of the customer's personal data and requiring the vendor to comply with the CCPA.

Key Considerations When Negotiating a DPA

When negotiating a DPA, many vendors will insist upon starting with the vendor's form DPA, which tends to be heavily drafted in favor of the vendor and may inadequately protect the personal data provided by the customer. Therefore, as the customer, it is important to carefully review and typically negotiate DPAs.

In addition to the legally required contractual obligations noted above, there are some additional provisions that the customer will likely want to consider adding to the DPA with the vendor. For example, these include:

- Requiring the vendor to comply with applicable U.S. data privacy laws;
- Imposing additional technical and organizational measures to protect personal data;
- Requiring vendor's assistance with investigation and remediation of a personal data breach at vendor's sole cost;
- Ensuring that personal data also constitutes "confidential information" under the related agreement;
- Obligating a vendor to maintain cyber insurance;
- Imposing an obligation upon the vendor to indemnify the customer for breach of the DPA and in the event of a personal data breach.

In negotiations of DPAs, contentious issues to negotiate often include the following:

- Indemnification obligations for the vendor's breach of the DPA and/or a personal data breach;
- Limitations of liability for breach of the DPA and/or indemnification obligations;
- The scope of audit rights (especially for cloud-based service providers), as customers often demand bespoke security audit procedures and/or the right to conduct onsite audits, whereas vendors often agree only to provide summaries of third party audits;
- Reimbursement of costs arising from a personal data breach; and
- Timing for notices in the event of a personal data breach, as customers often seek notice 24 hours after a vendor reasonably suspects a personal data breach, whereas vendors often agree to provide notice only 72 hours (or longer) after confirming a personal data breach.

Other Data Privacy Considerations for Vendor Management

Finally, customers should keep in mind that DPAs are not the only way that they should or must manage vendors. Prior to engagement, customers should conduct diligence of a vendor's privacy and security practices. Selecting an inadequate vendor that triggers a consumer lawsuit, personal data breach, or regulatory violation may cause reputational and commercial harm. Pursuing a breach of contract claim against the vendor that violates a DPA cannot rebuild trust with customers or repair a damaged brand name. In addition, smaller or less sophisticated vendors might agree to a customer's DPA requirements but have no practical means of meeting those requirements. Absent a strong insurance requirement, such vendors would likely be incapable of making the customer financially whole in the event of a breach of the DPA, which makes selecting the right vendors critical.

Once a DPA is in place with a vendor, customers should exercise their negotiated audit rights and monitor for updates to the DPA. The CCPA provides a strong incentive for exercising such rights, as customers that annually exercise such right are not responsible for the vendor's violation under the CCPA. Lastly, it is important to monitor developments in data privacy laws and enter into any necessary amendments to the DPA to ensure the parties compliance with relevant data privacy laws.

Footnotes

---

[1] California (the California Consumer Privacy Act, as amended by the California Privacy Rights Act), Colorado (the Colorado Privacy Act), Connecticut (An Act Concerning Personal Data Privacy and Online Monitoring), Delaware (the Delaware Personal Data Privacy Act), Florida (the Florida Digital Bill of Rights), Indiana (Senate Bill 5), Iowa (Senate File 262), Montana (Consumer Data Privacy Act), Oregon (Senate Bill 619), Tennessee (the Tennessee Information Protection Act), Texas (the Texas Data Privacy and Security Act), Utah (the Utah Consumer Privacy Act), and Virginia (the Virginia Consumer Data Protection Act).

[2] Senate Bill 370.

[3] The Washington My Health, My Data Act.

[4] According to the Federal Trade Commission, financial institutions must enter into agreements with vendors that include "security expectations, build in ways to monitor [the] service provider's work, and provide for periodic reassessments of their suitability for the job."