BURR FORMAN LLP

Checklist for Addressing Data Privacy and Cybersecurity with Your Vendors

Article
05.15.2023

RELATED PROFESSIONALS

India E. Vincent, CIPP/US, CIPM

RELATED CAPABILITIES

Cybersecurity & Data Privacy

In our last newsletter, we discussed due diligence as it relates to selection of vendors. The second part of that exercise is to negotiate your agreement with the vendor to properly manage any risks you identified. In this article, we will touch on some of the key provisions that should be in agreements with your vendors and some tips for negotiating those provisions.

The Vendor Agreement

Frequently, vendors will present standard contracts for products or services, but because data privacy laws are constantly changing, those contracts may not have been updated to address the most recent data privacy or cybersecurity considerations. Even if the agreements do address those issues, they may do so in a very cursory manner that fails to provide protections that may be necessary for your business, or they may not address a particular law or regulation to which your business is subject. Taking the time to negotiate the data privacy and security provisions in these agreements can save a lot of headaches in the event of a security incident, but it is also considered part of the required standard of care under certain data privacy laws.

Definitions

Defining the terms may seem obvious, but if contracts have not been updated to address privacy and cybersecurity concepts, the definitions required to address the security concepts may be missing. A few definitions that are needed in most contracts involving data processing include:

Checklist for Addressing Data Privacy and Cybersecurity with Your Vendors

- What is "personal information"? What is "sensitive personal information"?
- What is "data processing"?
- What is a "data breach" or a "security incident"?
- What is "anonymized/deidentified data"? What is "aggregated data"?

Compliance with Laws

Many vendor agreements include a standard compliance with laws provision that requires both parties to comply with all applicable laws. The agreement should make it clear that "all applicable laws" includes all data privacy laws that your business must follow. Defining the data privacy laws that are encompassed in the applicable laws is particularly important if your business is subject to laws of jurisdictions other than the state whose law governs the contract.

Standard of Care

In most agreements where the vendor will process data, the customer should include language that expressly requires the vendor to meet a certain standard of care when collecting, using, storing, sharing or destroying personal information and other confidential information. In some cases, the customer's industry may dictate those standards and in others it may be the customer's internal standards. It is important for the customer and vendor to agree on the appropriate standard of care.

In most cases, that standard of care requires the vendor to at least:

- Maintain the confidence of all personal information,
- Use the personal information solely to perform under the agreement,
- Have written agreements with similar requirements with any third parties that will have access to the personal information as a result of the vendor's actions; and
- Implement and maintain security measures consistent with standards in the industry.

There are several variations of each of these requirements that may be considered in appropriate circumstances, such as requiring consent before a particular subcontractor is granted access to data, and those variations should be considered and implemented as appropriate.

Vendor's Policies / Procedures

If the vendor has its own security policies and procedures in place, and the customer determines those policies and procedures to be adequate, the vendor agreement should require the vendor to maintain these policies, plans, and procedures throughout the term of the agreement. It should also require that those policies and procedures be reviewed and, if necessary, updated on at least an annual basis.

Checklist for Addressing Data Privacy and Cybersecurity with Your Vendors

Safeguard

The vendor agreement should require the vendor to maintain appropriate administrative, physical, and technical safeguards necessary to meet the standard of care required to protect the vendor's and the customer's systems and the customer's data. For businesses operating in a regulated industry such as financial services, health care, or payment processing, maintaining the safeguards required by the industry specific regulations should be a requirement of the agreement. For customer – vendor relationships that carry a high degree of risk, it may be desirable to expressly state the minimum safeguards that are required, rather than specifying a general standard that must be met.

System Documentation

The customer may include a contractual requirement for the vendor to maintain documentation of its information technology infrastructure identifying all systems, end-points, system connectivity, access control measures, backup or redundant servers, and permitted access through each end-point. If the vendor does not already have such documentation in place, discussions around the level of risk posed by the vendor's access to the customer's data and systems can help identify the appropriate level of documentation that needs to be generated and maintained.

Security Breaches

Because the vendor is responsible for the security of the customer's data, there are certain responsibilities the vendor should have in the event of a breach to ensure that both the vendor and the customer can meet their legal obligations. First and foremost, the vendor needs to contain and remedy the security breach, but at the same time, the vendor needs to provide timely notice of the incident to the customer so that the customer can assess any notice or reporting requirements and ensure that it is able to meet all of its obligations under the data breach notification laws. Recognizing that it can be difficult for the vendor to focus on notification requirements in the midst of a security breach, it is important for the customer to understand its legal reporting and notification requirements in order to guide the time frames in which the vendor must notify the customer.

In most cases, the customer, who is likely the data controller under laws that identify the parties in that manner, should have the discretion to confirm whether or not there has been a breach with regard to the customer's data, whether or not notification is required for individual consumers, employees, governmental agencies, or others, and whether or not any offerings should be made to the affected individuals, usually in the form of credit monitoring and/or identity theft protection. Because the customer also has the incentive to maintain relationships with its customers or employees, most contracts will restrict the vendor from notifying anyone of the breach without the consent of the customer, unless the vendor has an independent legal obligation to do so.

Although the discretion to make these determinations about the incident frequently lie with the customer, vendors are usually required to assist with the investigation and assessment efforts, and in some cases to cover the costs of notice and any remediation offerings. In order to ensure that the customer has the information it needs to make determinations as to whether there was a breach, whether notice is required,

Checklist for Addressing Data Privacy and Cybersecurity with Your Vendors

and whether any remedial offerings should be made to affected individuals, customers may want to include a contractual requirement for the vendor to provide the customer with access to all logs, reports, records, etc. regarding the incident.

Indemnification

In conjunction with standard indemnification and limitation of liability provisions in the vendor agreement, these concepts should be considered with respect to the data privacy and cybersecurity obligations. Most parties will negotiate who should have liability for the costs associated with a data breach, with significant weight placed on where the breach originated. If either party is responsible for the damages incurred by the other party, the agreement should address whether any stated caps on liability apply to data privacy and cybersecurity damages, whether there are any increased caps on liability for data privacy and cybersecurity damages, or whether there are no caps on liability for data privacy and cybersecurity damage.

Security Compliance

Because security requirements and best practices are changing on a regular basis and because it is easy for a system to move out of compliance with stated requirements over the course of time, many vendor agreements provide the customer the opportunity to conduct annual audits of the vendor's security posture or require the vendor to respond to an annual security questionnaire from the customer.

Insurance

In a market where it is becoming hard to obtain affordable cyber-insurance, and the coverage provided by the policies is far from standard, most customers still feel it is worthwhile to require the vendor to have such insurance. The coverage limits and types of coverage can vary significantly depending on the vendor's line of business and how sophisticated its current security systems are. Because of this, it is important for both parties to have an understanding of the types of cyber insurance that are most relevant for their industry and the particular customer – vendor relationship so that the insurance requirements can be appropriately tailored for the situation.

Conclusion

These are some of the key considerations for vendor contracts that appear in almost all customer - vendor relationships, but there will be additional or differing risks for many situations. Considering the scope of work to be performed by the vendor and selecting the appropriate security standards for that scope of work is important for protecting both the customer and the vendor.

If you could use some assistance determining what type of security requirements to include in your vendor contracts, or if you are a vendor and would like assistance incorporating these provisions into your agreements on a proactive basis, feel free to contact a member of our Cybersecurity and Data Privacy team or other Burr & Forman attorney with whom you work.