CARLTON FIELDS

Privacy and Cybersecurity Perils in Hastily Signed Work-From-Home Vendor Contracts

April 01, 2020

COVID-19 spurred an overnight surge in demand for work-from-home vendors. These include companies offering audio and videoconferencing services, cloud services, e-commerce platforms, and virtual desktop infrastructure, to name a few.

Companies without preexisting relationships with such vendors may have had no choice but to rush out and enter into agreements in order to keep their businesses running. But doing so without fully considering privacy and cybersecurity concerns could expose the business to unnecessary risk. Even companies with long-standing contracts in place with these types of vendors may find those contracts outdated and in need of renegotiation.

Whether entering into new contracts with work-from-home vendors or renegotiating old ones, businesses should address the following questions that may stem from hastily signed contracts occasioned by the COVID-19 pandemic.

1. **What Data Is Being Collected, How Is It Being Used, and What Is the Nature of the Relationship With the Vendor?**

The business should consider whether the vendor will have access to personal information, confidential business information, or other sensitive information, and what the vendor's contract or policy says it can do with that information. Vendor-side contracts and privacy policies tend to provide vendors with wide latitude in how they can use personal information collected from you, your customers, or your employees. And, often, these contracts are offered on a take-it-or-leave-it basis.

In addition to evaluating the extent to which the vendor can access, use, or sell the information transmitted via the vendor's platform, the business should consider its corresponding legal obligations with respect to the vendor's collection and use of that data. This analysis can be difficult given the wide variation in how "personal information" is defined, and how those variations may affect the obligations placed on businesses and vendors for securing, using, and transferring such data. Individual rights (like the right to delete or opt out) conferred by the European Union's General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA) may apply to the information that is the subject of the contract. A hastily-agreed-to contract may not fully account for that reality.

Indeed, businesses subject to the CCPA should consider whether the vendor qualifies as a "service provider" under the act. We have discussed the qualifications of a "service provider" under the CCPA previously. To qualify as a "service provider," the personal information at issue must be necessary for a "business purpose" as defined by California law. Cal. Civ. Code § 1798.140(d). Also, the vendor contract itself must contain certain language, including a restriction on the vendor's ability to sell, retain, use, or disclose the personal information inconsistent with the CCPA. The contract must also contain a certification that the vendor knows, understands, and will comply with its CCPA obligations.

Failing to do so may mean the transfer of personal information to/from that particular vendor in exchange for its services may be considered a "sale" under the CCPA, triggering the act's stringent opt-out and notice provisions. This is true even if the business is not exchanging data for money.

2. **Does the Business Need to Update Its Privacy Policy?**

The business must be sure to update its privacy policy to reflect the data flows involving this vendor. This may mean revising the business's privacy policy following the execution of the contract to detail a new category or type of personal information being collected, or sharing taking place with a new class of vendors.

The business may have to revise further its privacy policy to reflect any language that the vendor contract itself may impose on the business. Certain vendor contracts require the business using the service to make certain disclosures of its own in its privacy policy, including that the business is using the vendor and a disclosure and link to the vendor's own privacy policy.

3. **What Happens If There Is a Cybersecurity Incident?**

The business should evaluate the vendor's cybersecurity practices and disclosures as to how it will safeguard the information its services collect and transmit, and what will occur in the event of a breach at the vendor concerning the business's data.

As an initial matter, the business should examine the contractual obligations of the parties as they relate to cybersecurity. The contract's terms should set forth the requisite cybersecurity standards that the parties will follow, including any third-party standards, and whether the business has auditing rights.

The contract should also include what will happen in the event of a "cybersecurity incident" at the vendor that impacts the business's information. These provisions may include prompt notice to the business, a cooperation and information-sharing requirement, and a statement about which entity shall make consumer notice should it be required. Be sure the definition of a "cybersecurity incident" in the contract is the same as, or close to, your information security team's understanding of the term. It should be sufficiently broad to include incidents that may not rise to the level of a data breach under state notification laws.

Moreover, consider whether the contract should include any additional obligations in the event of a "cybersecurity incident," such as cost-transfer or indemnification based on causation or a requirement of ongoing, post-termination cooperation. These are all terms that are best negotiated at the time of contracting rather than in the heat of a suspected data breach. And these terms might be overlooked in the rush to execute a contract to facilitate working from home.

4. **What Are the Terms for Service Cancellation or Interruption?**

Since COVID-19, the time and attention spent on force majeure clauses has naturally increased. Care and attention should be spent understanding the terms for canceling the contract. Can the vendor terminate the contract based on events specified in the contract, such as pandemics, without cause or with minimal notice? Can the business?

Likewise, the business should consider whether the contract promises uptime levels or percentages of uninterrupted service. As entire workforces shift to working from home, that has placed unusual stress and high demand on technology, making system interruptions more likely. The vendor contract should provide the business with some certainty. Knowing this in advance can help the business plan for interruptions and add certainty in uncertain times.

Work-From-Home Vendor Contract Checklist

- Does the contract reflect your understanding of what information the vendor is collecting, using, and transferring in providing the service?
- Does the vendor qualify as a "service provider" under the CCPA?
- Does employing this vendor trigger any GDPR obligations?

- Does the business need to update its privacy policy to reflect the new vendor relationship?
- Do you need to update your privacy policy to reflect new data flows involving the vendor or obligations from the vendor contract?
- Does the contract reflect applicable cybersecurity standards and include breach notification provisions?
- Does the contract define the events that may trigger the cancellation of service and provide for a certain level of uptime?

Authored By

John E. Clabby

Patricia M. Carreiro

Related Practices

Cybersecurity and Privacy
Technology
Business Transactions

Related Industries

Technology