ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Negotiating Data Privacy in Multivendor Technology Contracts

Compliance and Ethics

Privacy and cybersecurity are evolving into a complex ecosystem of compliance, especially for technology. Is there personal data? Should individuals have the right to opt-in or opt-out of the processing of their data? Is the data being transferred across borders? Does the General Data Protection Regulations (GDPR) or new privacy laws in Nevada or California apply?

An onslaught of bewildering questions will arise based on business needs, applicable laws, relationships involved, and technology available. It is a struggle for companies to simply keep up, much less anticipate how to guard against future changes.

In this environment, counsel must advise their company about compliance while nevertheless enabling the implementation of business objectives. One area where this is particularly difficult is multivendor arrangements. These arrangements integrate services and technology from multiple vendors.

There are many practical reasons that are beyond the scope of this discussion that could persuade your company to choose this approach over a single vendor solution or in-house development. For example, the multivendor arrangement may result in technology that is cost-effective, best-in-breed, and scalable.

As a result, the multivendor approach has grown in popularity. While it has many benefits, one downside is that privacy and cybersecurity risks are often more complicated, as the number of risks increases with the number of vendors. For example, data mapping must map data across multiple entities.

Put simply: The vendors in these arrangements depend on each other as well as the customer to

provide their piece of the technological jigsaw puzzle. One vendor, for example, may depend on another for secure encrypted data transfers, which demonstrates a key risk for the company; the company is dependent on the integrated products and services of the vendors for success, and one vendor's failure to perform services for another can be a liability for the company.

The keys to addressing future privacy and cybersecurity risks in a multivendor arrangement lie in effective procurement, contract negotiations, contract administration, and company policies. Each contract will bring legal considerations, privacy and cybersecurity practices, technological strengths and weaknesses, relationships with other vendors in the arrangement, and business objectives specific to a particular vendor.

To the extent that you achieve company stakeholder buy-in, future-proofing the arrangement by integrating the parties into a single network is essential to implementing new compliance requirements quickly and with minimal disruption.

Contracting process

In a multivendor arrangement, your company is integrating a jigsaw puzzle of entities, products, and services as well as privacy and cybersecurity requirements and practices. As the customer, you should consider negotiating each vendor agreement simultaneously with the other vendor agreements or, if this is not possible, executing contracts with the same key privacy and cybersecurity terms.

The terms should focus on anticipating a dynamic rather static relationship among the vendors. To this end, customers should negotiate with each company to obtain the same coordinated governance, change management, and incident management process.

It is easier to negotiate these objectives at the same time when you may have the leverage rather than later when you do not. A patchwork of different rather than coordinated obligations will make current terms and future changes difficult to administer.

Contract terms

To future-proof the contracts, you should specifically negotiate terms anticipating compliance obligations will change by including the following:

- Vendors are required to follow the company's expressed prior written instructions about processing data.
- Vendors are required to comply with amended terms reflecting the customer's response to changes in law.
- There are terms obligating the vendor to sign additional agreements as required by law.
- The remedies the customer has, if the vendor or vendors fail to comply, are sufficient.

Each of these terms will help with complying with future changes in the law that impact the arrangement, but obtaining these terms will be subject to the company's bargaining power.

Cooperation, coordination, and communication

You may want the vendors to work together to address changes in privacy and cybersecurity with

you, but in practice, this is harder to accomplish than it may seem. Including language in the agreement that says that the vendor will comply with laws and follow your instructions is a good start, but it may not be sufficient.

Terms that obligate cooperation, coordination, and communication among the vendors are critical to avoid finger-pointing related to, for example, a data breach or a violation of current or future privacy requirements. There are many ways to ensure that vendors do not engage in finger-pointing. One approach is to have the vendors sign a cooperation agreement. The cooperation agreement can either bind all parties, or, depending on bargaining power, may be non-binding.

Cooperation, coordination, and communication should include providing information as required by the other vendors or the customer to comply with privacy and cybersecurity laws; working with other vendors and the company in connection with changes in privacy and cybersecurity laws; and good faith discussions about reducing any costs related to changes in compliance obligations.

A good example of when cooperation, coordination, and communication are critical is when a data breach happens. Each vendor should be brought into a single incident management process for the arrangement. When data is moved and processed from one entity to another, the risk of a data breach increases. Management of the processing of data from one entity to another is consequently vital.

In many jurisdictions, companies are obligated to notify regulators, individuals, or other parties of a breach within a certain timeframe. It is important to have a plan in place to manage the investigation, containment, reporting, and remediation of the breach among the vendors after the event. This will require that you include a clear assessment of third-party risk and change management related to changes in the law.

Third-party risk and change management

At the outset, even before negotiations with the vendors, it is important for the company to identify through its vetting process its risk tolerance for the arrangement. It will be difficult in the privacy and cybersecurity ecosystem to be certain about what future risks may arise. One can speculate that these risks will likely fall into two buckets: data rights management (e.g., consent, the right to be forgotten, or data portability) and cybersecurity.

However, lawmakers and courts are finding new requirements to impose. Once a company determines its tolerance for reputational damage, fines and fees, remediation, class actions, and private rights of actions, third-party risk management (TPRM) will help manage the multivendor risks more effectively. Within the TPRM framework, you should expect to address the following questions:

- What data will be processed, who will process it, where the data will be processed, how the data will be processed, and why will it be processed?
- Are the responsibilities and roles of each vendor regarding data and cybersecurity clearly articulated? Which laws, regulations, and standards are applicable?
- Are vendors complying with their responsibilities, including coordinating, cooperating, and communicating about changes in privacy and cybersecurity?
- Can you hold the vendors accountable for failures to make changes?

A joint governance process can help resolve changes in privacy and cybersecurity risks in a coordinated fashion, and, thus mitigate the risks posed by future changes.

Liability and cost traps

The liability and cost traps related to multivendor arrangements and a failure to future proof against an evolving privacy and cybersecurity ecosystem comes in several forms. For example, vendors may only agree to comply with those laws applicable to the service provider and exclude those that are not.

Counsel must take care to understand the consequences of agreeing to vendor contract language, especially where vendors are linked by dependencies in a multivendor arrangement. Poorly understood terms may result in additional costs if new data processing obligations will require changes in business practices or technology.

Implementation and/or maintenance of the integration of technology and services among vendors may be higher if you must pay the cost of developing a work-around related to compliance. This cost may be unavoidable, but it is important to be aware that you will need a larger budget than initially projected if this occurs.

It is also important to identify how changes in the law may impact caps on liability. To some extent, it will be impossible to fully determine liability between you and the vendors or between the vendors. It may also be difficult to obtain uncapped damages.

However, as you may have discovered with potential fines of up to four percent of global revenues under the GDPR or class action damages under the CCPA, it is important to assume your liability may grow. To the extent possible, given commercial realities and bargaining power, it is important to negotiate the best cap possible.

Privacy by design

The recommendations above attempt to integrate the principles of privacy by design into procurement, contract negotiations, contract administration, and company policy for technology-driven multivendor arrangements. This is perhaps the best tool you will have in future proofing your multivendor arrangement in an evolving privacy and cybersecurity ecosystem.

Craig Young

Corporate Counsel

a Fortune-500 legal department

Craig Young is corporate counsel in a Fortune-500 legal department. He focuses on global technology, commercial contracts, intellectual property, and data privacy. He is CIPP-certified by the International Association of Privacy Professionals in EU and US privacy. He is a graduate of Georgetown University Law Center and the University of Virginia.