ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Privacy Now: Is Your Company Willing to Gamble on Vendor Management?

Technology, Privacy, and eCommerce

Vendor management is a recognized risk — and one that is growing larger every day. As counsel, we may be involved with vendor management on several fronts. Take these four areas: due diligence, contracting, lifecycle management, and termination. In this article, we will look at notable laws and review how they affect vendor management, examining how in-house counsel can protect their companies from undue risk.

Laws impacting vendor management

The European Union's General Data Protection Regulation (GDPR)

Managing risk has always been a standard corporate activity for companies, but the prevalence of hosted outsourcing in the past two decades has increased that risk. When GDPR was enacted in 2016, the extraterritoriality provisions quickly became a concern for companies around the world. GDPR requires controllers (those who determine how data is processed) to exercise control over processors (those who are hired to process data on behalf of the controllers) and in turn subprocessors (those who the processors hire). The penalties for non-compliance are high: potentially four percent of gross revenue worldwide.

The data protection authorities have been quite active in enforcing GDPR — with the known fine amounts so far more than €284 million, with the highest single fine being €50 million against Google by the French CNIL (Commission nationale de l'informatique et des libertés). The most common

violations are insufficient legal bases for data processing and insufficient technical and organizational measures to ensure information security. The most active regulator has been Spain with 236 fines, followed by Italy with 79, although Italy has issued the highest total amount of fines (total fines €76 million), averaging nearly a million euros per fine.

Companies should also note that the European Economic Area, which encompasses Norway, Iceland, and Liechtenstein (in addition to the European Union), has adopted GDPR.

Selected resources on the European Commission's New Standard Contractual Clauses

Check out a selection of resources regarding the new standard contractual clauses adopted by the European Commission on June 4, 2021, regarding the transfer of personal data under the European Union's GDPR.

The United Kingdom’s General Data Protection Regulation

With the United Kingdom out of the European Union, it adopted its own version of GDPR. The provisions addressing the individual Member States have been removed, but most of the other requirements are the same. Thus, the requirements of GDPR towards vendors (processors and subprocessors) are in place for the United Kingdom as well.

With this, organizations that appointed the UK Information Commissioner’s Office (ICO) as their lead data protection authority (DPA) for Europe should now have appointed a new DPA in the European Union or vice versa. Make sure to establish relationships with the ICO if the selected DPA was in another country, appointed a representative in the European Union and United Kingdom as applicable if not physically established in one or both locations, and implemented data transfer mechanisms from both locations. A prior Privacy Now column addressed the requirements.

In the United States: California, Virginia, Colorado

In the United States, the current state-level omnibus privacy laws have nearly identical requirements to control vendors: the CCPA (California Consumer Privacy Act), its successor the CPRA (California Privacy Rights Act), and the Virginia CDPA (Consumer Data Protection Act). Companies are accountable for the actions of vendors or third parties they engage. These laws overlap with strong sectoral laws such as the Health Insurance Portability and Accountability Act (along with its subsequent amendments, HIPAA) and seem to be a strong indicator of the diverse omnibus laws arising on the state level.

In California, certain contractual requirements must be met if you want your vendors to be service providers. If those contractual requirements are not met, the vendors will be considered third parties, triggering additional compliance needs. These requirements are not specified in the CCPA as a section clearly labeled “Vendors” like GDPR’s article 28 on processors (Chapter 4 in general addresses controllers and processors). In the CCPA, the requirements are listed in the definitions of “service provider” and “third party” in section 1798.140(v) and (w) respectively.

The CCPA contractual requirements are:

- Processing personal information for a business purpose specified in a written contract,

- The contract prohibits the vendor from selling, retaining, using, or disclosing the personal information for any other purpose than what is specified or those operational business purposes permitted under the CCPA, and
- A certification that the vendor understands these restrictions and will comply.

Once the CPRA takes effect in 2023, contracts will have additional requirements, including defining "sharing" and "sensitive personal information." It will also include contractors alongside service providers. Counsel should review the new requirements and determine how best to migrate current agreements over the next 18 months.

Virginia, on the other hand, approaches controllers and processors in a way that resembles GDPR. Like the CPRA, it takes effect in 2023 and includes the concept of sensitive personal information, but does not include a one-year look-back on individual rights.

The most recent state to (maybe) pass an omnibus privacy law is Colorado. On June 8, the Colorado Privacy Act was passed by both houses and now awaits the governor's signature to become law. Normally he would have ten days to sign, but since the legislative session is over for 2021, he has thirty days to sign or veto (Colo. Const. Art. IV, Section 11). If he does not do either, it becomes law by default. If passed, the effective date will be July 1, 2023 as long as there is no referendum petition filed. If there is, then the law and its enforcement date are subject to election protocols. Like Virginia, which follows GDPR, it incorporates the concepts of controller and processor and has specific contractual requirements and obligations.

Oversight needs

With the shift from on-premise solutions to cloud-based solutions, software as a service (SaaS), Platform as a Service (Paas) and Infrastructure as a Service (IaaS), companies are more dependent than ever third-party services. The concepts of controller and processor are not necessarily aligned with how companies do business, but they are concepts that are likely to remain for quite some time. In general, ensure that your data or the data entrusted to you by your customers remains secure. The laws mainly address personal data, not corporate data, but where you can make sure all data is secure, you should do so.

Before engaging and partnering with a vendor, it is critical to make sure you take the appropriate steps to protect your business — from customer data to corporate secrets to legal compliance. Below are some of the basic steps of a vendor oversight process. Each of these should be approached from a risk-based perspective, which means identifying where you are comfortable not acting and where there may be significant consequences if the risk is not addressed.

Due diligence

Due diligence comes in all flavors. From the financial stability of the vendor to whether they are processing the data you provide in a country whose government surveillance laws run afoul of the European Union's guidance, it is up to in-house counsel to conduct their due diligence alongside the various departments that own the pieces of the vendor activities.

From the privacy or data protection side, privacy and security risk assessments should be performed. The issues to determine are the appropriate level of inquiry, whether you accept documentation they provide or conduct your own assessment, and how to determine where the risk outweighs the benefit.

For the latter, you will need to make sure the business units that want to use the vendor understand that there is no such thing as guaranteed approval.

Contracting

Contracts have always been a delicate issue. With so many contractual requirements, the process is becoming even more complex. Identify the terms that are non-negotiable for your company, such as indemnification or limitations of liability, and preferred (but more flexible) terms. This may also depend on each side's bargaining power.

For privacy or data protection requirements, one or more appendices may be needed to accommodate various jurisdictional requirements, especially if your company is subject to the GDPR or HIPAA. For US state laws, incorporate those jurisdictional requirements into the contract itself or into a relatively simple data processing agreement or addendum.

Additionally, if privacy or security concerns have been identified, it is possible to contractually require third parties to implement certain measures within a certain timeframe. For example, perhaps they need to acquire cyber-liability insurance within 90 days or seek ISO 27001 / 27701 certification within 18 months. This is a common way to address risks that you would like to see mitigated, but which the business considers the vendor worth the risk.

Management

Controlling your risk via vendors is not a once-and-done process. You need to evaluate their performance over the life of the relationship. Part of this includes ensuring they are fulfilling their duties, but part is also making sure the risk profile has not increased. Based on the services or products they provide, you may want to do an annual re-evaluation before renewal so that you have leverage to encourage mitigation of identified elements. You can choose to re-evaluate every two years — or never — depending on the risk. If they are handling personal data or corporate secrets, never is not ideal.

In addition, note when certain required mitigation steps, such as the insurance coverage or the certification, need to be executed. This is especially important if there is a data breach and it turns out they have more data than you knew. Also note that you should require them to have incident response processes and to notify you quickly when one occurs.

Lastly, make sure there are processes in place to be notified if their scope of activities has changed. Scope creep is a common, but significant risk.

Termination

Whether the end of the relationship is voluntary or not, amicable or not, there needs to be termination processes. It is best to negotiate this beforehand when the parties are on good terms rather than at the end when they might not be. It may not be possible or feasible to return your data, but they should be able to destroy it and provide certification of having done so. If they are not able to destroy it due to a reason to retain it, have them document the reason and identify a time when they can destroy it.

Determine your risk appetite

Vendor relationships are a fantastic way to supplement the expertise and services your company needs to be effective, efficient, and robust. But they come with risks. The risks aren't necessarily complicated to address, but they do take time, attention, and diligence. Start with your risk appetite and determine if your company can gamble on a vendor going wrong in a large and public way.

K Royal

Global Chief Privacy Officer

Crawford & Company

K Royal earned her JD from the Sandra Day O'Connor College of Law at Arizona State University. She also holds a PhD in Public Affairs from the University of Texas at Dallas.

Reach out to K about her column at @heartofprivacy on Twitter, or www.linkedin.com/in/kroyal/.