May 16, 2025

Leah A. Druckerman, Julia Tama and Rob Hartwell

Smoothing Privacy Contracting: Six Ways to Reduce Friction in Data Processing Agreements

4min

Negotiating a data processing agreement (DPA) is typically a necessary step when engaging vendors that handle personal data. However, these negotiations have become time consuming and complex, given the evolving privacy landscape. Drawing on Venable's experience, here are six ways for customers (controllers) and vendors (often processors) to streamline DPA negotiations and close deals faster.

1. Keep Your DPA up to Date

Whether drafted by customer or vendor, a template DPA is a necessary document for addressing legal requirements under privacy laws, and it should be reviewed and updated as privacy laws change. An outdated DPA not only fails to satisfy applicable laws but may necessitate additional negotiation and undercut a partner's confidence in your company's privacy compliance.

2. Be Practical and Reasonable in DPA Legal Terms

An effective way to reduce negotiation time is to begin with a well-drafted, market-aligned DPA or checklist for reviewing counterparty DPAs. Aggressive, impractical, or one-sided terms may seem protective for your organization, but in practice they are likely to be rejected. Avoiding them from the start helps reduce redlines and builds trust with counterparties.

Some common friction points include:

- **Short Security Breach Notification Deadline.** Most laws require a vendor to notify customers of a security breach "without undue delay," and imposing a very short deadline may be impractical and provide little marginal benefit to the customer, because there is not enough time to gather necessary information to meet both parties' legal obligations.
- **Audit Rights.** Audit rights are required by most privacy laws, but avoiding onerous terms like unlimited on-site audits can help close a deal. Consider a tiered structure. For example, start with questionnaires or reviews of certifications (ISO, SOC, etc.) and escalate to more invasive audits only after certain triggering events or where strictly necessary to meet legal compliance requirements.
- **Subprocessor Engagement.** Many privacy laws require customer approval for the vendor's use of subprocessors. These laws provide two options: prior written consent or an opportunity to object. The latter is easier for vendors and provides comparable protection for customers.
- **Commercial Risk Allocations.** Many customer DPAs include

uncapped or high liability limits, security breach cost-shifting, and indemnity rights, while vendor DPAs may include restrictive liability caps. These risk allocations are often contentious and require escalations. Consider the reasonableness of these terms and develop fallback positions. In some cases, it may be better to leave risk allocations in the master agreement.

3. Develop a DPA Playbook and Establish Escalation Paths

Develop a playbook that outlines your negotiation positions, fallback language, and risk tolerances on key provisions. This empowers your legal and procurement teams to negotiate efficiently and consistently, reducing the need for escalations to the privacy team.

Where escalations are necessary, define escalation paths to reduce turnaround time and improve consistency. Business, IT, security, and product teams are often consulted during DPA negotiations, and identifying decision makers and communication lines in advance speeds up approvals.

4. Know Your Data Flows

Before entering negotiations, conduct a privacy assessment and/or data mapping exercise to understand what data is being processed, how it is being used, and the purposes it is being used for. This allows you to answer questions from counterparties quickly and

propose terms that accurately reflect the risk profile and nature of the processing.

5. Maintain a Subprocessor List

For vendors, maintain and regularly update a list of subprocessors, including descriptions of the services provided, processing activities, and locations of processing. Sharing this list proactively helps preempt questions and shows a level of preparedness and transparency that customers appreciate.

6. Consider a Cover Sheet

If your organization takes unusual positions or requires an unusual term in your DPA, consider providing an explanation in a cover sheet. This helps set expectations, forestall objections, and convey the message that the company is thoughtful about privacy.

For example, most customers assume that the vendor is going to act as a "processor." However, some types of services cannot be provided by a "processor," or a vendor may need rights to use data for its own purposes, such as training AI models. Explaining these positions in advance can help reduce negotiating time.

No Time Like the Present

By following the tips above, companies can improve their efficiency and close deals faster—without sacrificing privacy obligations. There is no time like the present to update and streamline your

DPA process.

Please contact Venable's privacy attorneys if you want assistance with applying these tips, improving contracting processes, or other aspects of privacy contracting. With the right approach, what was once a legal bottleneck can become a competitive advantage.

Related Services

Practices

Privacy and Data Security

Related Insights

States Ramp Up Enforcement of Privacy Opt-Out Compliance

3min

September 17, 2025

Businesses Should Upgrade Privacy Compliance Programs for New State Laws in 2025

4min
