4 Creative Strategies for Negotiating Data Protection Agreements

Commercial and Contracts

Intellectual Property

Technology, Privacy, and eCommerce

Data protection remains a rapidly changing area of the law, with material seemingly updated monthly. The divergent approach taken by various jurisdictions only further complicates an organization's compliance. This varied and changing landscape means that approaches to drafting or negotiating data protection agreements (DPAs) have also changed, even since the ACC IP network's 2019 article on the topic.

Parties are also often misaligned on a DPA's purpose, slowing down the contracting process. For example, proposed changes to the parties' audit rights and limitation of liability caps in a DPA may be a surprise to parties that believe material commercial terms are finalized.

For some organizations, a DPA is primarily a compliance tool (e.g., to ensure an organization acts as a service provider or processor). For others, a DPA must fulfill any commercial or operational objectives and is critical to operations if the company must establish data rights for providing or improving its services.

1. Providing notice and transparency

Obligations to comply with the law (whether mutual or favoring the party drafting the DPA) are standard in DPAs. If the parties must cooperate or rely on the other for achieving compliance, however, a mere agreement is likely insufficient for ensuring that both parties achieve compliance.

Lawfully collecting certain types of data, such as biometric or vehicle location information, may require both the technology customer and vendor to collect consent from and provide notice to data subjects (i.e., the person(s) to whom the information relates).

If the technology customer has privity with the data subjects, the vendor must affirmatively require the customer to take certain actions (such as providing the vendor's notice to data subjects) for the

vendor to comply with law.

As a point of caution, parties should avoid agreeing to provisions requiring one party to inform the other of legal obligations arising under the DPA and/or the underlying activity. Doing so might constitute providing legal advice, for which neither party should be responsible (a technology customer has not retained its vendor as counsel or vice versa).

2. Scoping and defined terms

At the negotiation's outset, parties should align on the DPA's scope. Often, parties have fully negotiated material terms, such as audit provisions, prior to entering into a DPA.

Parties may remove those provisions to streamline the negotiation and avoid rehashing previously negotiated provisions. Moreover, pointing out that provisions are redundant to an underlying agreement is one argument upon which the party with less leverage may use to strike burdensome provisions.

The types of provisions included in the DPA, however, do not solely determine a DPA's scope. How the DPA defines key terms such as "personal data" or its equivalent term will substantively determine the parties' rights and obligations. Looking for subtle changes to those defined terms will help ensure the DPA's substantive provisions have full effect.

As an example of one such change, vendors might look to define personal data only as information that the customer provides to the vendor, even though the vendor directly collects personal data on the company's behalf.

Restrictions on the vendor's use of data, for example, should also apply to the data directly collected by the vendor for the vendor to act as a processor or service provider. In sum, be sure that defined terms align with your organization's classification and data, the intended and/or prohibited use of the data, and the particulars of the parties' relationship.

3. "Mandatory terms" in DPAs, a list that keeps growing

In 2019, parties focused primarily on terms required by the EU's General Data Protection Regulation (GDPR) and had begun to consider the CCPA. The privacy compliance landscape has changed in the past two years, especially for US-based technology customers or providers, and your partners' positions have likely adapted to these changes.

For example, Virginia and Colorado passed comprehensive privacy laws set to take effect in 2023. Those laws (in line with GDPR) establish the roles of controller and processor and emphasize that determining whether a party acts as a controller is a fact-based inquiry. Therefore, parties must ensure that DPAs accurately reflect which parties determine the purposes and means of processing (and thereby act as a controller) instead of reflexively relying on boilerplate language to declare that a technology provider is a processor.

> How the DPA defines key terms such as "personal data" or its equivalent term will substantively determine the parties' rights and obligations.

Updated guidance from the European Union and California Attorney General may also restrict technology providers' right to act as processors/service providers.

Given that changing landscape, legal departments must work with procurement departments to establish an organization's compliance position, i.e., when the organization acts as a controller or processor and when it requires contractual counterparties to do the same. As the role of some technology providers may change from processor to controller based on the legal developments mentioned above, moreover, parties must use creative strategies if compliance positions conflict.

One such example would be if a technology customer relied on a technology provider to act as a processor or service provider for the customer to avoid CCPA's (or the Colorado and Virginia law's) definition of sales, but the technology provider believes that it acts as a controller or business.

Strategies for resolution include, among others, deploying a consent for sharing the personal information or narrowing the scope of information transferred (i.e., masking any personal data so only deidentified information is shared, avoiding the privacy laws' scopes).

4. New standard contractual clauses, Brexit, and transatlantic data transfer issues

Parties execute the Standard Contractual Clauses (SCCs) alongside or as an attachment to virtually all DPAs that involve transatlantic data transfer. During the summer of 2021, European authorities (an EU-wide regulator called the European Commission) released new SCCs. The new SCCs (among other changes) require parties to re-evaluate form DPAs and even DPAs executed in the past that remain in force.

Parties must make decisions about how to implement the new SCCs before implementation, whereas the prior SCCs did not provide parties with much choice about how to launch the terms.

> To avoid risks of the DPA's invalidation, parties should also update DPAs to clarify that the SCCs shall control in the event of any inconsistency between the two documents.

For example, the new SCCs permit parties to choose any EU Member State for the SCCs' governing law and place for dispute. The new SCCs also require parties to select an appropriate "module" within the clauses depending on whether the parties act as controllers or processors. As one marked improvement from the prior clauses, the new SCCs contemplate (and provide a module for) transfers from processors to controllers (Module 4).

The new SCCs' introduction may also require changes to the body of DPAs. For example, parties may not cap liability under the SCCs, so liability caps in the DPA or other applicable agreements should contain a carve out for liability arising under the SCCs to avoid conflicting terms.

To avoid risks of the DPA's invalidation, parties should also update DPAs to clarify that the SCCs shall control in the event of any inconsistency between the two documents.

As always in the area of data protection, parties must stay flexible when it comes to SCCs. As one final example of the rapidly changing legal landscape shaping DPAs, we note that new Model Clauses for transfers out of the United Kingdom are on the horizon, as UK regulators plan for their

release in early 2022.

Stacie Greskowiak McNulty

Director and Counsel

HOPE Cape Town USA

Stacie Greskowiak McNulty is director and counsel of HOPE Cape Town USA. She most recently served as general counsel for Orbital Effects/R2 Space, a private company providing cutting-edge radar satellite technology and related applications to the United States government. She also previously served as senior legal counsel and director of litigation at Marconi Group/PanOptis, where she developed and executed highly successful global litigation strategies in patent infringement cases, contract and commercial disputes, and competition matters.

Farah Cook

Partner

Kilpatrick Townsend & Stockton, LLP

Farah Cook is partner at Kilpatrick Townsend & Stockton, LLP. She concentrates her practice on technology-focused commercial agreements, marketing technology arrangements, advertising technology, and licensing of intellectual property, strategic alliances, content distribution, and innovative cloud and data products.
Her combination of in-house and big law firm experience, as well as her broad practice, gives her the ability to creatively and efficiently identify, understand and navigate issues in technology, commercial and marketing matters.

John Brigagliano

Associate

Kilpatrick Townsend & Stockton, LLP

John Brigagliano is an associate at Kilpatrick Townsend & Stockton, LLP. Brigagliano focuses his practice on data privacy compliance, biometric technologies, e-commerce, electronic signatures, technology licensing and procurement, and cross-border transactions. In particular, Brigagliano structures data privacy compliance strategies and efficiently resolves CCPA and GDPR compliance hurdles for companies across a variety of industries.