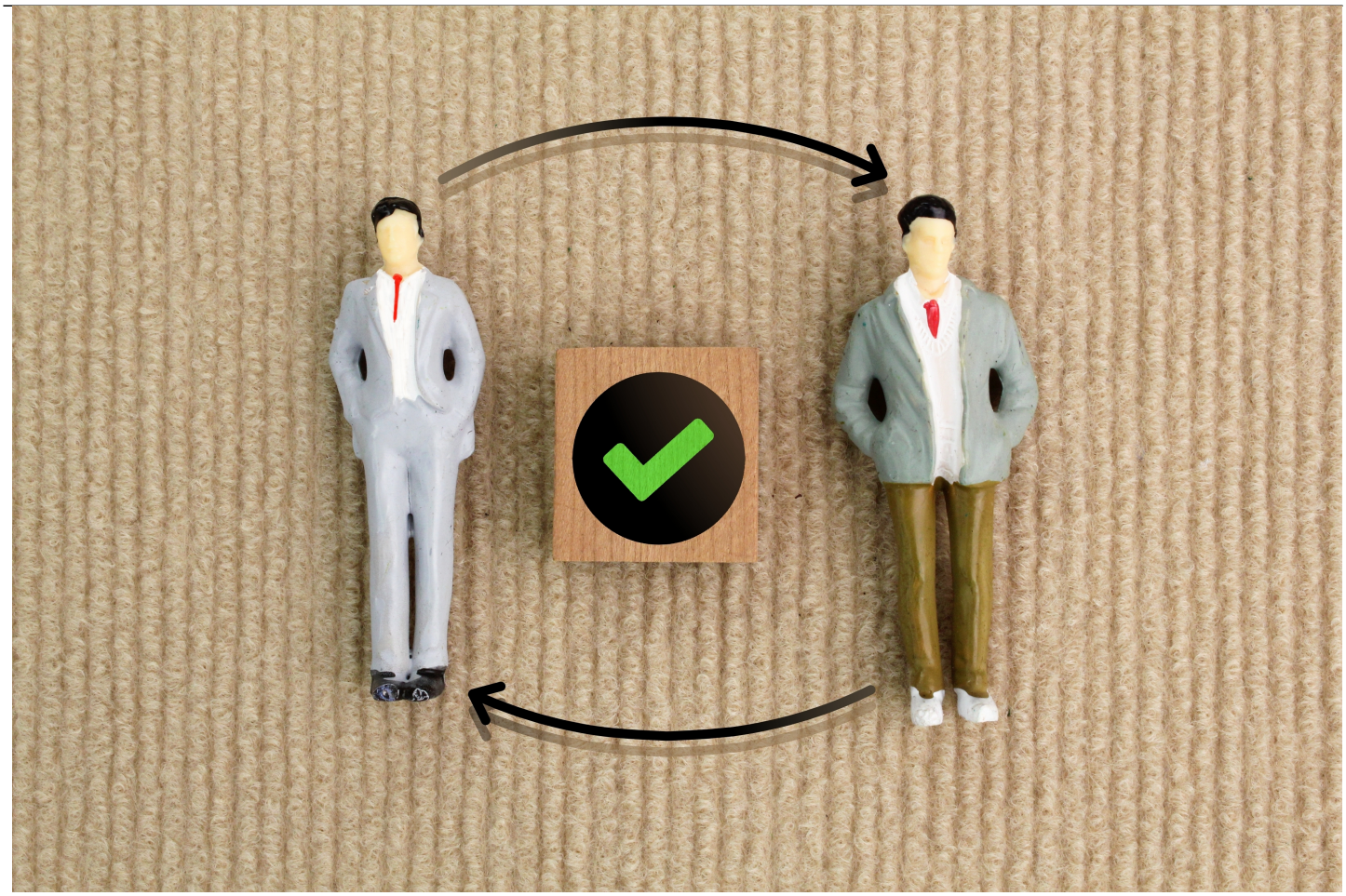
ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Legal Considerations: Procurement Contracting

Commercial and Contracts



Banner artwork by Fauzi Muda / *Shutterstock.com*

This is the third part of a multi-part series addressing best practices and experience of a legal and procurement team in a dynamic startup environment.

The first two articles in this series (Procurement's Power Duo: Finance and Legal and A Perfect Pairing: Automation and Performance Reporting) address the interplay between finance and legal during the procurement process. This article focuses primarily on the legal terms and process of procurement contracting. In this article, "buyer" refers to the purchasing entity (typically your organization) and "vendor" refers to the party providing product or services to the buyer.

So you want to buy a product or service, and you have engaged with the finance department and gone through the sourcing and financial approval process to purchase it. Now it is time to negotiate the contract terms for the purchase and related order forms and other documentation.

Non-disclosure agreements

Before initiating any exchange of confidential information, it is imperative to execute a non-disclosure agreement (NDA) between the buyer (your company) and the vendor. This step protects confidential information, fosters more open and effective conversations throughout the buyer-vendor relationship, and ensures a clear legal framework in the event of a contract dispute or security incident. Where mutual, the NDA also enables the vendor to share information more freely with the buyer, expediting any transaction.

To streamline this process, buyers should flex their purchasing power (aka “the power of the purse”) by starting with NDA terms already agreeable to the buyer, a concept commonly referred to as “pushing your paper.” However, larger vendors with inherently more market power may insist on utilizing their own vendor NDA templates.

It is important to educate your business owner (internal stakeholder) on confidentiality protocols such as clear confidentiality markings on buyer data or content and potential use of clean rooms or named-party access for particularly sensitive data, to avoid potential trade secret contamination and unauthorized access to data.

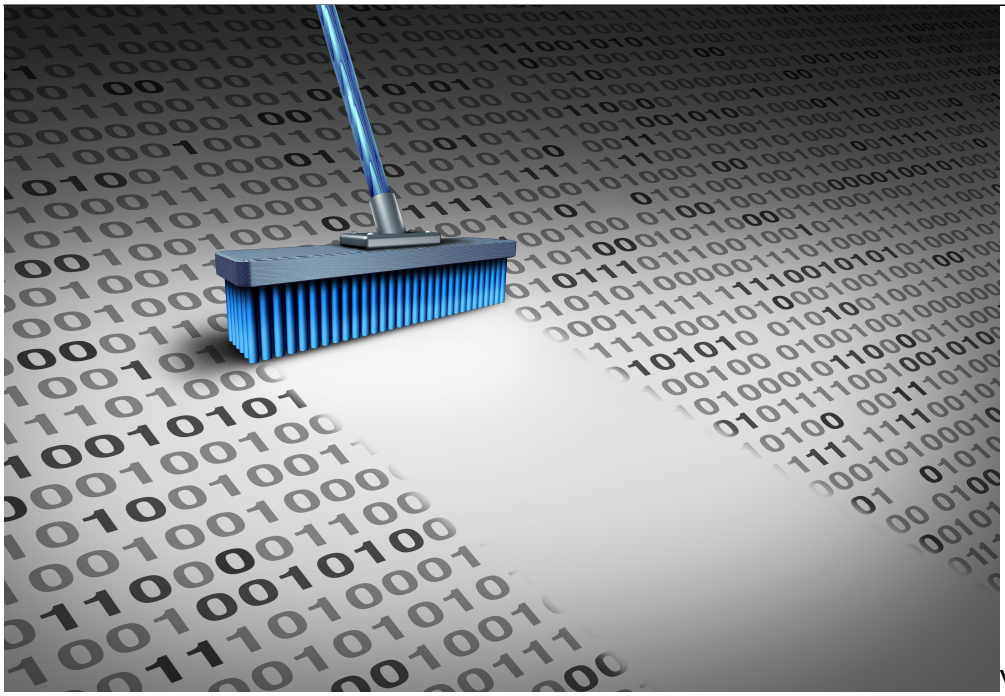
It’s not just about price

Data portability

Since the buyer is putting data into the vendor’s tool (often a software as a service, or SaaS, platform) in many instances, the buyer should require a contract clause regarding the return of company data at the termination or expiration of the contract. A buyer should never see their data “held hostage” by a vendor who makes it difficult to export the data in a standard format or who charges an exorbitant export fee. Buyers should negotiate up front the terms for exporting of data and the format in which it can be exported, to avoid a “vendor lock-in” type situation where the data is stuck in a particular vendor’s platform and cannot readily be retrieved, giving undue leverage to the vendor.

Data deletion upon termination

Any vendor who holds confidential or personal information of the buyer’s expands the potential attack surface, and thus, the risk to the buyer. If a vendor has a security incident, for example, and exposes the buyer’s data, this would become the buyer’s problem and potentially requires the buyer to notify their own customers (and employees) of the data incident.


Vendors are responsible for returning or removing any stored data of the buyer. Lightspring / *Shutterstock.com*

Some vendor contracts place the onus on the buyer to request deletion of buyer data upon contract termination. However, from the perspective of privacy and security, the onus should not be on the buyer to notify the vendor that they want their data returned or destroyed, but rather on the vendor to proactively return and/or destroy any buyer data held, according to the wishes of the buyer as negotiated in the agreement. Buyers do not need the headache of a data incident caused by a former vendor who held onto data longer than necessary. The buyer should consider negotiating a time limit, typically 30 – 60 days after the termination or expiration of the contract, for the vendor to return and/or delete all stored data of the buyer, and certify this in writing to the buyer.

Privacy protections

The buyer should require a Data Processing Addendum/Agreement (DPA) if the vendor processes personally identifiable information (PII) of data subjects, particularly so if the data subjects are residents of jurisdictions where a data protection agreement is required (European Union, United Kingdom, Brazil, China, Dubai, India, Saudi Arabia, South Africa, Thailand, Turkey, and various states in the United States). Prior to contracting, the buyer's legal and business teams should know the type of data (e.g., confidential, personal, or sensitive information, such as financial or health data, etc.) shared with the vendor, and the duration and nature of vendor usage of this data, and review the contract accordingly.

Where possible, the buyer should conduct an information security (InfoSec) review on any new vendors, and potentially on renewal for any vendors who may have a change to their business situation, including verifying if the vendor has security and privacy certifications (e.g., ISO 27001 and SOC 2).

Availability and uptime

Vendors generally promise the sun, moon, and stars, but it is up to the buyer to ensure that the vendor delivers and, if not, to have a clear mechanism for terminating the contract. The buyer may want to require a service level agreement (SLA) for the vendor's service. If the buyer's business is seasonally dependent (e.g., large sales volume during holiday periods) then the buyer may require that uptime will be prioritized during these rush periods.

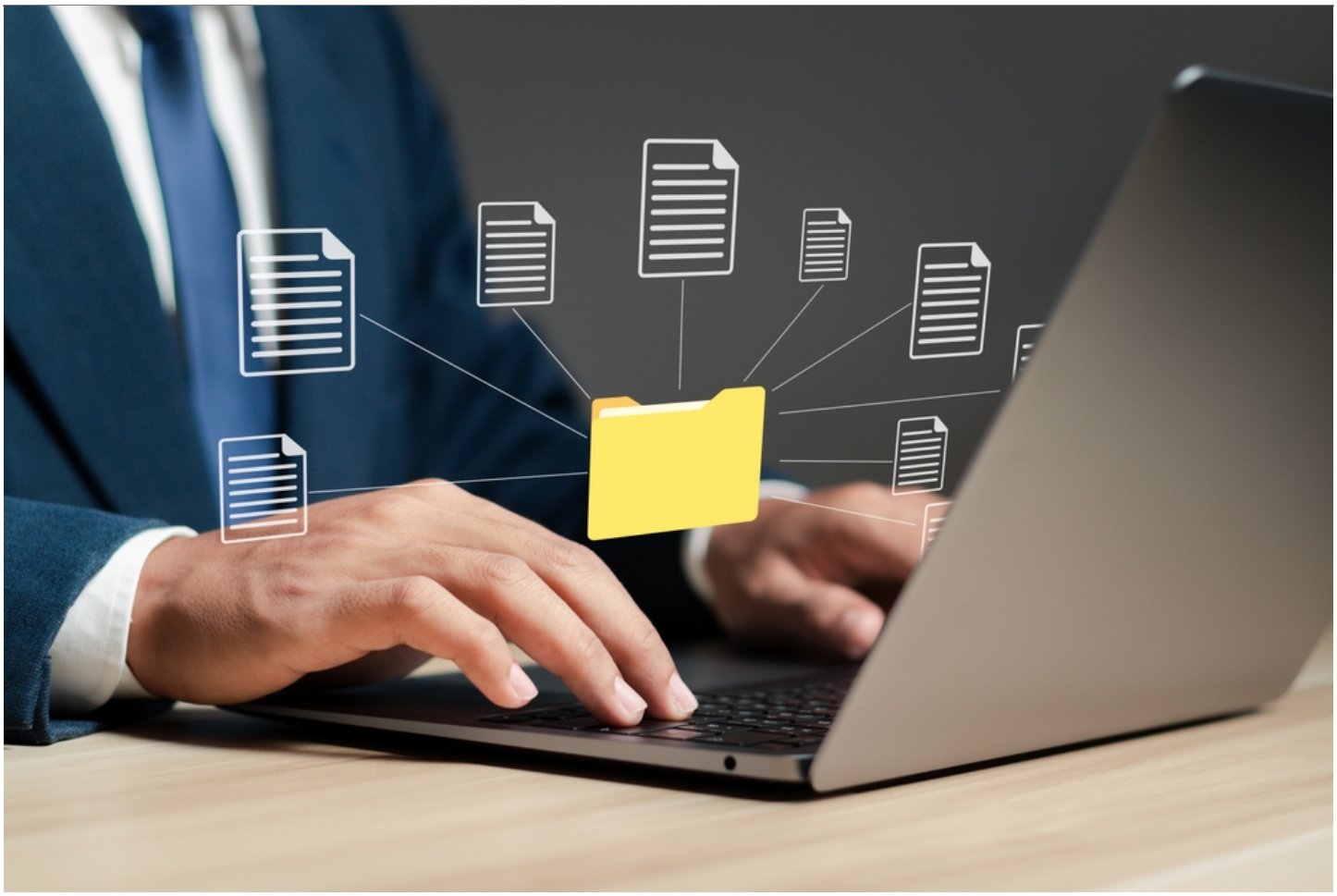
> Vendors generally promise the sun, moon, and stars, but it is up to the buyer to ensure that the vendor delivers and, if not, to have a clear mechanism for terminating the contract.

Ownership of and rights to use data

Whenever the buyer shares data to the vendor, there should be clear guardrails around ownership and what if any rights the vendor has to use or retain such data. Generally the buyer's data should only be used by the vendor for the purpose of the agreement and for the term of the agreement. Any vendor rights to use the buyer's data should be revocable by the buyer. If the vendor retains data, such retained data should be anonymized or de-identified, and only retained as aggregated data that cannot be tied back to an individual data subject.

Surprise! Your contract auto-renewed

When vendors and business owners constantly change due to company growth or contraction, this can result in an auto renewal "merry-go-round," especially when business owners may not be fully engaged in managing their vendors and renewals. Often, prior to establishment of a formal contract or procurement database to track renewal dates and deadlines for non-renewal notices, a missed non-renewal deadline can force the buyers into an additional undesired period of spend with a vendor, simply because the company failed to get out in time. From an early stage, buyers should maintain a detailed record of tools purchased, their expiration dates, the business function or owner, whether an auto-renewal is part of the agreement, the utilization level of the tool, and any deadline for notice to not renew.



When auto-renewal is part of an agreement between buyers and vendors, detailed records should be kept and maintained to prevent missing non-renewal deadlines. A9 STUDIO / *Shutterstock.com*

To avoid auto-renewals, prior to signing a purchase, buyers should negotiate with the vendor to opt out of the auto-renewal. The buyer may delete “shall automatically renew” and “— days notice for non-renewal” language and instead state that “upon prior written approval by both parties, this agreement or statement of work may renew for a successive term.” This allows the buyer to evaluate at the end of the term whether the business need for the tool is still there and, if not, provides an easy way out of the contract. When a vendor knows that they need to earn a renewal, the vendor is more likely to provide the buyer with a higher quality of service.

Price caps

There is another layer of protection the buyer may request: capping any price increase in subsequent renewals. From the vendor perspective, agreeing to a price cap ahead of time provides predictability to the buyer and, so long as the vendors perform well, this reduces the likelihood of the buyer shopping around for other vendors. Without a price cap, then ahead of an upcoming renewal, the buyer should request quotes from alternative vendors, so the buyer is not jammed with a sizable price increase on renewal. Offering a price cap to the buyer helps secure the vendor’s footprint and potential renewal opportunity with the company.

> Offering a price cap to the buyer helps secure the vendor’s footprint and potential renewal opportunity with the company.

One year at a time

Generally a buyer should stick to annual agreements or negotiate the ability to terminate a multi-year contract early, particularly if the vendor service is not as promised, or if the buyer later determines that the service is no longer needed.

As an alternative, if a buyer does agree to a multi-year agreement with a vendor (often in return for preferable pricing terms), the buyer should request a “gated annual structure” with a price agreed for subsequent years, but with written approval being required prior to each subsequent year term starting. This provides price protection for the buyer and a smooth transition from one year to the next if the buyer so desires, and keeps the vendor on their toes to satisfy the buyer.

Easy in, easy out — ensuring you can cleanly exit contracts

Virtually all contracts provide for termination in the event of an uncured material breach by either party. However, the specific conditions for termination and any refund (often prorated, usually from date of termination) can vary considerably. Often the buyer can negotiate the terms of the refund and from which date the refund starts. When working with a new vendor, particularly one without a long market history, the buyer should negotiate a termination for convenience clause. This is a backstop in the event of unsatisfactory service, failure to meet milestones, or significant issues with the product purchased from the vendor. While vendors don’t like such terms, the buyer may instead request it for the first 90 or 180 days while the product or service is being used for the first time, and to motivate the vendor to assist with a successful deployment or setup.

A termination for convenience clause may be implemented early on contingent upon poor service. Nuttapong punna / *Shutterstock.com*

Limitations of liability and what really matters

Limitation of liability is a key section in any procurement agreement. The vendor generally wants to keep it as tight as possible, and the buyer generally expects it to be sufficiently broad to cover real (or perceived) risks the buyer faces when contracting and sharing buyer data (particularly confidential information or personal data) with the vendor.

The vendor may attempt to cap liability for any data incidents, often at fees paid for the prior 12 months. However, the buyer must determine if 12 months of fees are sufficient to cover damages resulting from such an incident. This depends on the spend by the buyer, the quantity and sensitivity of information shared by the buyer to the vendor, and often the jurisdictions in which the buyer is operating.

The buyer may request uncapped damages for certain types of data, but generally vendors refuse this. There is often a middle ground via a super cap (e.g., three or five times the amount of damages or sometimes more of a regular liability cap) for confidentiality or privacy incidents relating to sensitive data. It behooves the buyer to at least request this rather than just accept the default 12 months of fees as a liability cap.

Indemnification and other battles

Along with limitation of liability, indemnification is a frequently contested area of procurement agreements. The buyer wants indemnification from the vendor for third party claims relating to the purchase, such as from an intellectual property assertion entity or competitor of the vendor. The vendor does not want to insure against every possible scenario, rather only those reasonably foreseeable and under the vendor's control. It is common for indemnification to flow both ways, where the buyer indemnifies for harm reasonably foreseeable to flow from the buyer's actions (e.g., a privacy or misuse of data claim against the vendor). From a perspective of fairness, the buyer generally should not indemnify the vendor for a broader set of risks or a larger amount than the vendor is indemnifying the buyer for. This depends also upon the nature of the data the buyer is providing to the vendor, and the industry the vendor operates in, and what the vendor is permitted to do with the buyer's data.

Prior to purchase, the buyer should conduct a thorough InfoSec review of the vendor product to help identify and mitigate risk from the vendor, including analyzing the scope of access which the vendor has to the buyer's data. If a vendor can access the buyer's customer data (i.e., a customer relationship management system), the buyer should ask for indemnification against foreseeable claims resulting from a data loss caused by the vendor.

Issues and opportunities beyond price and use of the service or product

Marketing goodies — press releases, customer testimonials

Vendors often include a right to issue a press release, publish the buyer's logo, gather and publicize testimonials, etc. as a standard term. However, these "goodies" should be earned by the vendor and not given away automatically. Keeping these goodies in reserve until a successful deployment is completed (e.g., 90 or 180 days after the terms starts) helps ensure the vendor actually delivers on what they promise.

> … "Goodies" should be earned by the vendor and not given away automatically.

Feedback

Vendors often include a clause with full rights to any and all feedback provided by the buyer. However, without a clear record of such feedback, such as feedback provided over the phone, who is to say definitively what the vendors will use? Thus, it is advisable to limit feedback clauses to “written feedback” to avoid disputes about what verbal feedback was provided or rights granted.

Non-solicitation

Vendors often include a non-solicitation clause, usually with a stiff monetary penalty attached. Buyers should generally refuse such terms or limit them as tightly as possible (limited duration, direct solicitation by a party working with the vendor, etc.) to avoid a situation where a recruiter at the buyer, unaware of the non-solicitation clause, reaches out to a buyer employee as part of a general recruiting campaign. Any non-solicitation clause should exclude general posting of job roles or hiring of any individual who applies to a publicly posted position where there is no direct solicitation.

Order form amendments

It is often faster and lower friction to make a small amendment as an “order form change” rather than having to send the whole agreement back for legal review. This is particularly true at peak periods like end of quarter.

The goal is a collaborative relationship

> Both buyers and vendors should partner to negotiate fair and balanced legal terms which address the needs and concerns of each party and pave the road for a fruitful and collaborative relationship.

Both buyers and vendors should partner to negotiate fair and balanced legal terms which address the needs and concerns of each party and pave the road for a fruitful and collaborative relationship. Such negotiations should be completed early in the process prior to the buyer’s team “falling in love” with a particular tool or service, which can lead to loss of leverage by the buyer.

Michael Moore

Chief Privacy Officer

Lacework

As chief privacy officer, Moore is responsible for privacy and cybersecurity, procurement, product counseling, transactional support, patents and intellectual property strategy, open-source software, and other matters. He is a seasoned attorney with more than a decade and a half of privacy, cloud, transactional, software and hardware counseling and patent and IP experience, which follows his technical career in logic design and software engineering. Moore holds the IAPP privacy qualifications of CIPP-US, CIPP-E, CIPP-C, CIPM, and CIPT. He is a graduate of the ACC Executive Leadership Institute class of 2014, and also part of the team winning the Association of Corporate Counsel Value Champions Award (2018) while at Pure Storage.

Lauren Norvell

Attorney

LG Intellectual Property, LLC

Lauren Norvell is a member of the California State Bar. Norvell's practice focuses on privacy and intellectual property matters facing technology companies. She has strong practical experience in international privacy laws and regulations. Norvell holds the IAPP privacy qualifications of CIPP-US, CIPP-E, and CIPM. Throughout her legal career, Norvell has supported in-house legal teams at various technology companies in Silicon Valley. Prior to enrolling in law school, Norvell worked at Apple, Inc. in the global security operations department.

Lauren McHugh

Contracts Manager

Lacework Inc.

Lauren McHugh is a Contracts Manager at Lacework Inc., where she excels in legal operations and contract negotiation. With a robust background in legal support and operational efficiency, she has streamlined workflows and developed innovative solutions to boost organizational productivity. Throughout her career, Lauren has played a pivotal role in supporting in-house legal teams at leading technology companies in Silicon Valley. She holds a degree from Santa Clara University, where she studied Political Science, Communications, and Spanish.