Data

How collaboration between privacy and contracting can optimize compliance

Photo: Getty Images

Chase D'Agostino | FTI Consulting, Linda Brust | FTI Consulting

August 26, 2026 • 3 min read

Working together, contracting and privacy teams help the organization stay compliant and adaptable, reducing future legal costs.

Data privacy compliance can no longer be treated like a siloed function. Laws like the California Consumer Privacy Act and the California Privacy Rights Act – among dozens of other US state and international data

partners.

With this evolution, oversight of contractual agreements with vendors that sit within an organization's data ecosystem has become a serious operational issue, and one that is often overlooked.

In many organizations, privacy and contracting teams operate on parallel tracks. Contracting teams focus on negotiating commercial terms, service levels, liability, and intellectual property, while privacy teams concentrate on data flows, retention, consumer rights and notice, and consent controls. Contracting teams likely own the negotiation process, but privacy teams provide the expertise needed to ensure the organization's data protection posture is accurately reflected within agreements.

The result of disconnects between these functions can lead to an array of problems. For example, an organization may enter into a vendor agreement that allows processing of sensitive information without assessment by the privacy team as to whether that processing is compliant with applicable regulations. Another is third-party partnerships that result in unapproved sharing of personal information.

Importantly, under California data protection laws, contracts are explicitly named as more than commercial frameworks. The regulation stipulates that vendor agreements stand as legal mechanisms that govern how data can be used, shared, and safeguarded. For example, requirements such as clearly defined "business purpose" limitations, restrictions on selling or sharing personal information, obligations for service providers and contractors, and audit and monitoring rights all hinge on precisely drafted contract terms.

general and CalPrivacy, formerly known as the California Privacy Protection Agency, alleged that entities failed to craft contracts that met regulatory requirements, resulting in multiple settlements exceeding $1.3m. These cases serve as stark reminders that demonstrable vendor and contract due diligence to ensure privacy requirements are upheld across the entire vendor environment is integral to avoiding violations.

When the contracting department serves as the central gatekeeper for vendor relationships, it is a natural and necessary partner to implement privacy requirements consistently and at scale across partner agreements.

Embedding privacy input early, ideally at vendor intake or during initial vendor evaluation, makes it easier for organizations to anticipate potential data privacy compliance issues that may arise in agreements, streamline negotiations, and avoid unnecessary problems downstream. A unified approach also maintains the same standards across all third-party relationships, creating consistency and reducing risk.

Joint frameworks between contracting and privacy teams can include:

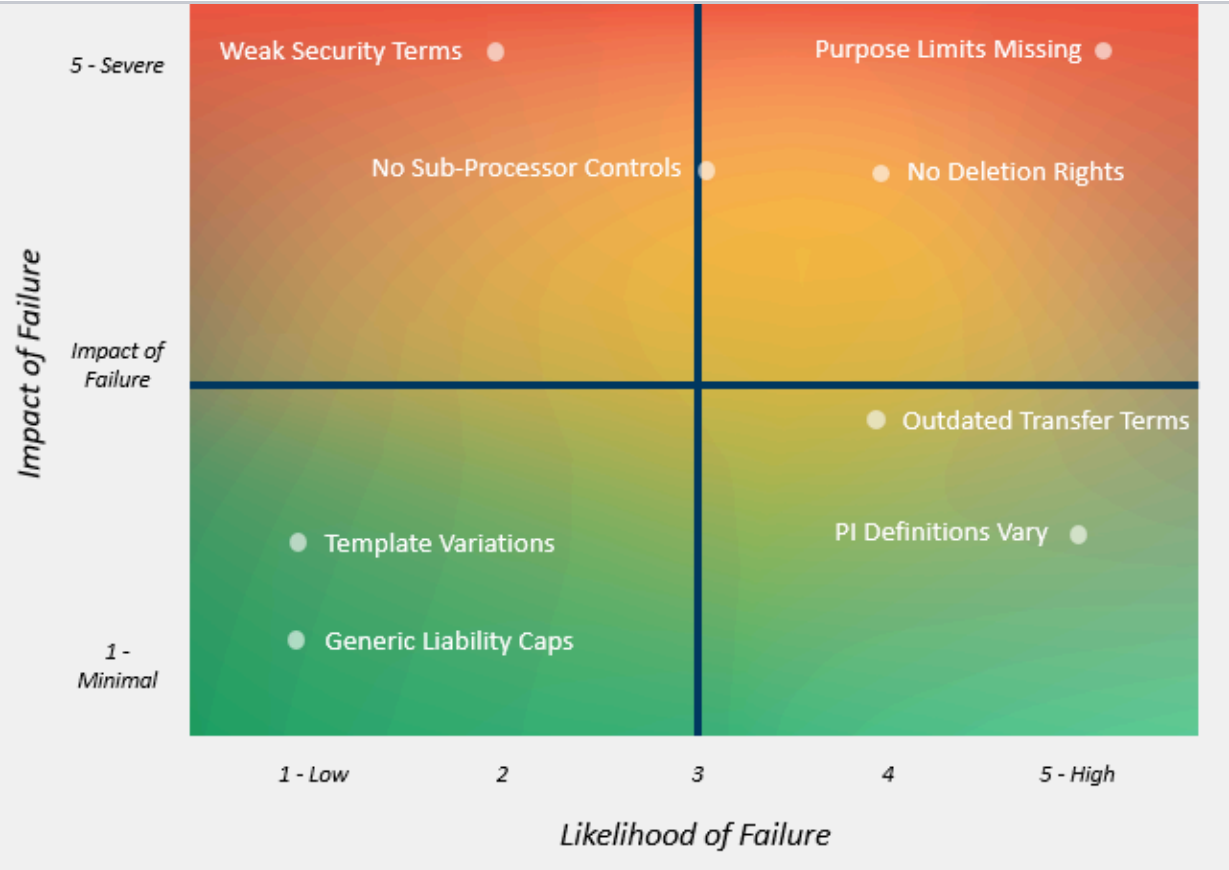
- standard data protection addenda with modular language to customize according to each vendor's unique attributes and functions;
- contract templates aligned with the requirements under California Consumer Privacy Act and all other applicable data protection laws;
- shared checklists or intake forms for consistent, repeatable, and efficient workflows so that contracts can be executed in a timely manner;
- centralized contract and vendor management systems to provide a single system in which contracting and privacy teams can

retroactively for legacy partnerships, and periodically for the entire relevant contract portfolio over time.

As privacy and contracting teams partner to intelligently assess their contract risks, the heat map below is a helpful reference to understand the correlation between privacy requirements, contracting gaps, and degrees of risk. Cross-functional teams can review agreements to identify where they fall on this scale, make strategic decisions about risk tolerance, and determine what remediation may be needed.

For example:

- Purpose limitation and no selling/sharing terms are the strongest controls against misuse of personal data.
- Security safeguards and incident notification directly reduce breach risks.
- Consumer rights support language is essential for operational processes and avoiding regulatory penalties.
- Sub-processor controls and audit rights help manage vendor-related risks.
- Contract templates kept up to date with regulatory language and organization-specific requirements



Impact of failure	*Likelihood of failure*
How severely a failure of this contract term would affect the organization's ability to meet privacy obligations, protect personal information, or withstand regulatory scrutiny. **High impact** = materially impairs compliance or creates significant exposure. **Low impact** = creates friction or inconsistency but does not meaningfully jeopardize.	How likely it is that this contract term is missing, weak, inconsistent, or unenforceable across the organization's vendor portfolio. **High likelihood** = commonly missing or inconsistent. **Low likelihood** = usually present or easier to enforce.

than treated as a final review step. Bringing privacy and contracting teams together through common governance, standardized workflows and scalable technology enables organizations to manage vendor risk more consistently while supporting business agility. A collaborative, risk-based approach allows privacy programs to evolve as organizations grow and regulatory expectations continue to change."

Data privacy laws have elevated compliance and contracting as critical functions that must be managed cross-functionally. Without coordination, important clauses may be omitted from vendor agreements or misinterpreted between parties, potentially resulting in compliance gaps that can be costly or operationally disruptive.

Seamless, strategic collaboration between contracting and privacy teams helps to ensure the organization remains compliant, agile, and resilient, particularly as state attorneys general and other authorities engage in insistent enforcement. When these functions work together, they help to reduce legal and operational risk, while strengthening trust, transparency, and robust governance.

Chase D'Agostino is the managing director with more than 15 years of experience serving global corporations and financial institutions; and Linda Brust is a director in FTI's Information Governance, Privacy & Security professional services team, FTI Technology.

New data obligations have come into force in the US. Here's what you need to do.

May 29, 2023

California's privacy regulator is looking into who collects, controls and shares the data your car is gathering from you as you drive.

August 2, 2023

Data

California Attorney General Rob Bonta targets mobile apps over privacy failings

Businesses with mobile apps that have failed to comply with the California Consumer Privacy Act (CCPA) have received letters.

January 31, 2023

Data

Organizations struggle to meet global data privacy laws

Only half of organizations are set to meet the legal requirements, says new report.

July 27, 2023