Mitigating Risk in Local Government Technology Contracts

By Nick Cotton-Baez, CIRSA Associate General Counsel

INTRODUCTION

Local governments greatly benefit from technological advancements in their day-to-day operations and the services they provide to their constituents and frequently turn to the vast market of third-party software and other technology products designed for local governments or similar entities. Local government standard contract forms and templates are often inadequate at addressing risks associated with technology products, and at ensuring vendor and local government compliance with laws respecting data privacy and security, intellectual property, and other cyber risks.

Consequently, local governments will often agree to negotiate agreements by use of the vendor's contract forms, only to find that the vendor is unwilling to negotiate substantive changes to its standard terms and conditions, which often heavily favor the vendor and do not recognize laws applicable to public entities. Local governments are then left with accepting the product on the vendor's terms and conditions or seeking an alternative product from another vendor who may be similarly unwilling to negotiate its standard terms and conditions.

However, some local governments have had success in negotiating changes to certain provisions of vendor contract forms, by creating narrow exceptions for specific risks and by citing laws applicable to local governments and vendors. This article is intended to familiarize CIRSA members with laws implicated by technology products, and provide information to assist members in their review and negotiation of contract terms with vendors for the purpose of mitigating liability risks. If you are a CIRSA member, you can also contact CIRSA's General Counsel Office for sample contract language, and your CIRSA Underwriting Representative with questions about cyber insurance coverages.

CONSIDER THIS SCENARIO

> Your Town[i] desires to purchase software for use at the Town's recreation center. The software program will allow recreation center employees to set up customer accounts and take payments of membership fees. To set up membership accounts, recreation center employees will collect customer names, addresses, phone numbers, email addresses, and credit card information ("customer information") and enter the information into the software. Customer information is then stored on remote servers owned by a third party through a separate contract with the software vendor. The software will allow members to book various fitness class offerings after they create a unique username and password. Additionally, the software utilizes an AI-powered chatbot (developed by a third-party) to assist with class bookings and other customer service items. The Town hopes to enter into a contract to use the software for 3 years. The vendor's standard contract form would cap the amount of damages the Town can recover from the vendor to fees paid to the vendor for the 12 months preceding a claim. This cap applies broadly, including to sums accruing under the vendor's obligation to indemnify the Town against liability for vendor's infringement of third-party intellectual property rights.

What to do?

First, it's important to recognize that software contract negotiations may require interdepartmental cooperation. While your recreation department will be the only department to use the software, your organization (as a whole) will bear the liability risks. If your organization has one, your IT department will be a great resource given their knowledge of the software business and industry standards related to software performance.

Second, you'll want to involve the organization's management and attorney in contract negotiations, as contracts for the procurement and use of software implicate a variety of laws and liability risks. Relevant laws include those aimed at protecting certain data from unauthorized disclosure, access and use, and increasing access to digital content for individuals with disabilities. Depending on the product, technology contracts might also implicate laws protecting consumers from harms related to bias in the use of artificial intelligence (AI) platforms and tools. To protect your entity from liability risks and statutory penalties, compliance with each of these laws must be addressed in a contract with the software vendor.

Third, local governments should carefully review and develop an understanding of the rights and obligations set forth in the vendor's form contract before executing the agreement or deciding to negotiate the provisions. As with other product and services contracts, local governments should closely review the form contract's liability shifting provisions, limitations and caps, and its indemnity and insurance provisions. Additionally, technology contracts often address intellectual property (IP) ownership and infringement, a service level agreement concerning the required amount of software uptime and allowed downtime, data backups, and rights concerning exchanged data.

Now, let's apply these laws and principles to the recreation software scenario.

Customer Data Privacy & Security

Our recreation center scenario involves the collection, storage, and disclosure to the software vendor of customer names, addresses, phone numbers, email addresses, usernames and passwords, and credit card information. Because the data set includes an email address and username in combination with a password that would permit access to the customer account, and credit card information in combination with a password that would permit access to the customer account, the information constitutes "personal information" protected under C.R.S. § 24-73-103. Under that statute, local governments have obligations to investigate and notify Colorado residents of known and suspected security breaches of their personal information and direct affected individuals to take steps to protect their compromised accounts. While the statute does not itself establish a distinct cause of action, it may create a duty for which local governments may be held liable for breaching.

The data disclosed to the vendor will also include customer names, addresses, telephone numbers, and personal financial information of past or present users of the Town's recreation center ("recreation user data"), which raises another issue under the Colorado Open Records Act, Section 24-72-201, et seq., C.R.S. ("CORA"). In general, CORA prohibits disclosure of this recreation user data (and similar user data for other services and programs), except in aggregate or statistical form so classified as to prevent the identification, location, or habits of individuals. Thus, your contract with the software vendor should ensure the vendor does not cause a CORA violation for which your organization would be held responsible.

Additionally, the recreation software will allow your customers to pay membership fees using a credit or debit card, triggering the applicability of the Payment Card Industry (PCI) Data Security Standard (DSS)[ii]. Your organization can face fines and suspensions of card processing privileges for violating the security requirements of the PCI DSS, even if caused by the vendor or vendor's software. Vendors providing software that takes credit and debit card payments will typically agree to the inclusion of a contract provision requiring PCI DSS compliance, as they're already required to comply with its security requirements.

In view of the laws discussed above, it's in your organization's interest to bind the vendor to security requirements and procedures to protect the personal information, recreation user data, and financial information contained in your data and to allow your organization to comply with its breach notification obligations under C.R.S. § 24-73-103. If your entity has an "incident response plan" related to technology security, consider attempting to bind the vendor to complying with it. Alternatively, while likely not directly applicable to the recreation software scenario[iii], your organization might look to the obligations of "third-party service providers" set forth in C.R.S. § 24-73-102 to inform the security procedures and practices you seek to impose on the software vendor through the contract.

Recall, in the recreation software scenario, customer data will be uploaded into the vendor's software and then stored on remote servers owned by a third party. This adds an additional layer of potential liability exposure for the Town at the server provider level. While it would be ideal to require the vendor to indemnify the Town against liability arising from the acts and omissions of the third-party server company—particularly because your organization will not have a choice in selecting, or a direct contract with, this third party—the vendor may be unwilling to agree to assume the liability of any third party for fear of being liable for causes beyond its reasonable control. In any case, it's in your interest to identify the third-party server provider and independently evaluate its security practices and procedures before entering into the contract with the recreation software vendor.

Data Usage Rights

Your organization should also consider the ways a vendor might use customer data for purposes other than fulfillment of your contract. Some vendor contracts may stay silent on this issue, or specifically authorize the vendor's ability to disclose, sell, copy, distribute, market, or allow third parties to access your customer data. In view of the laws discussed above and other privacy considerations, it's in your organization's interest to prohibit the vendor's use and disclosure of your customer data, except as necessary to fulfill its contractual obligations. Furthermore, it's prudent to require the vendor to disclose the third parties to which your customer data will be provided for purposes of fulfilling the vendor's contractual obligations, and mandate that the vendor require such third parties to handle your customer data with at least the same degree of care and protection as required of your vendor under the contract.

Accessibility

Under Colorado's technology accessibility law[iv], local governments are required to comply with statewide accessibility standards for individuals with a disability[v], in the creation and publication of online content and materials. The accessibility standards apply to both public external-facing and internal-facing information and communication technology (ICT)—such as software, applications, and websites—that is procured, developed, maintained, or used by local government entities. The law's coverage extends to third-party software forming part of a local government's ICT, and liability for noncompliance lies with the public entity that manages the content or platform.

Your organization may be subjected to statutory fines or held civilly liable for monetary damages if your ICT violates the accessibility standards, and thus it's important to ensure software is compliant before entering into a contract for its use. This, of course, requires due diligence prior to selecting a software program and executing a contract with a vendor for its use. Many local governments include in their requests for proposals (RFPs) requirements and questions regarding vendors' ability to comply with accessibility standards and deny awards to vendors that cannot assure compliance.

If a vendor assures its software is accessible in response to an RFP or otherwise, it's important to reiterate that assurance as a representation and warranty in the software contract. It's further protective to seek an indemnity from the vendor in case the vendor breaches the representation or warranty. While it may prove costly or difficult to enforce a vendor obligation to indemnify the local government for causing the local government to incur statutory fines, it's in your entity's interest to include such fines within the breadth of the vendor's indemnification obligation.

Intellectual Property

It's likely the software vendor's form contract will address intellectual property (IP) rights. If the vendor is licensing its IP to your entity, it's appropriate for the contract to include an agreement to indemnify you against suits claiming the vendor's software infringes on third-party IP. However, vendor contracts will often cap the vendor's total aggregate liability under the contract by reference to the amount of fees paid to the vendor under the contract. While the software vendor may be unwilling to remove liability caps in full, their form sometimes will—and from your perspective should—exempt damages

for IP infringement from the liability cap. It's in your organization's interest to negotiate the exemption if it's absent from the vendor's form.

Artificial Intelligence

Beginning on February 1, 2026, developers of high-risk artificial intelligence systems will be required to comply with new Colorado laws designed to protect consumers from any known or reasonably foreseeable risks of algorithmic discrimination in the high-risk system. See Senate Bill 24-205, codified at Part 17, Article 1, Title 6, C.R.S. (the "Act"). The Act also imposes obligations on entities "deploying" high-risk intelligence systems, which may apply to vendors whose software incorporates artificial intelligence tools that are developed by third parties to perform certain tasks, and possibly to local governments that license the software incorporating the AI tools.

Recall, the recreation software scenario contemplates a 3-year contract, which if executed in 2025 would extend beyond the Act's February 2026 implementation date. While it's unlikely the AI-powered chatbot integrated into the recreation software would constitute a "high-risk artificial intelligence system"[vi] under the Act—because the chatbot does not make "consequential decisions"[vii] and is intended to perform a narrow procural task of assisting with class bookings and other customer service items[viii] —it's important to become familiar with the requirements of the Act that are applicable to local governments ahead of upcoming implementation date.

Local governments have other interests when it comes to the integration and use of AI systems, including compliance with the data security and technology accessibility laws discussed in the sections above. Thus, it's prudent to consider protections for the customer information entered into the chatbot interface. For example, you might attempt to prohibit the chatbot from eliciting PII or financial information, or require the vendor to place a warning within the chatbot interface that users should not submit any PII or financial information. For more on this, check out this CIRSA article concerning the risks associated with the use of generative AI in local government operations.

Indemnity & Insurance

Using contract language to require vendor compliance with the various laws implicated by technology products is an important component of protecting your organization against risk. But it's not the only one. Your contract should also expressly obligate the vendor to indemnify your entity, its officers and employees, against claims and liabilities arising from the vendor's noncompliance with such laws. Furthermore, to help ensure there are financial resources backing these requirements, it's important to require the vendor to carry insurance of types and in amounts sufficient to cover its indemnification obligations under the contract and to protect against risks arising from the vendor's work.

More specifically, in addition to usual requirements that a vendor carry commercial general liability and workers' compensation insurance, your contract should include requirements that the vendor carry cyber risk insurance. Your contract should require that this coverage respond to claims and liabilities arising from the vendor's contractual duties and provide coverage for, among other risks, security breach, system failure, data recovery, business interruption, cyber extortion, social engineering, infringement of intellectual property, invasion of privacy violations, release of PII, payment card liabilities, and other risks. In addition to claims and expenses for liabilities to third parties, the contract should require that the vendor's coverage pay for breach response costs, regulatory fines and penalties, and credit monitoring expenses.
While coverage afforded to CIRSA members includes a sub-limited amount of first-party and third-party cyber coverage—unless the member has purchased a separate policy—it's standard practice and fair to require software vendors to carry their own insurance coverages that protect against liabilities and expenses arising from the vendor's own acts and omissions. If you have questions about CIRSA's cyber coverages, contact your CIRSA Underwriting Representative.

Contract Termination

Finally, in crafting any software or technology contract, your organization should consider its termination rights under the contract, and what happens to customer or other data in the event the contract is terminated or expires by its terms. It's in your interest to require the software vendor to destroy your customer and other data following contract termination, as you could still face liability if lingering personal information is accessed through a breach of the vendor's software after the contract terminates or expires. However, following termination, you probably won't be able to access customer information within the software (unless you've separately saved the information on your own system). Thus, upon termination, it's in your interest to require the vendor to return your customer information to you in a usable format (e.g., .csv, .txt, json, or hdf5 files) before the vendor is obligated to destroy it.

CONCLUSION

By familiarizing yourself and your organization with the laws and principles discussed in this article, you can help protect your organization from legal and liability risks associated with software and other technology products. While you may not have success in obtaining the most protective contract provisions on all of the matters discussed in this article, your increased knowledge of the applicable laws and potential liability risks will give your organization a fighting chance in contract negotiations!

If you have questions about this article, or would like samples of contract provisions of the type discussed in this article, contact CIRSA's Associate General Counsel, Nick Cotton-Baez, at nickc@cirsa.org.

Note: This article is intended for general information purposes only and is not intended or to be construed as legal advice on any specific issue. Readers should consult with their entity's own counsel for legal advice on specific issues.

---

i. While a town is used in the scenario, the laws and principles discussed in this article are also applicable to cities.
ii. The PCI DSS is a global standard for safeguarding payment card details to prevent fraud and data breaches, consisting of a set of security guidelines that mandate how entities must protect cardholder data, including credit and debit card information, when storing, processing, or transmitting it.
iii. The term "third-party service Vendor" covers entities contracted to maintain, store, or process personal identifying information (PII) on behalf of a governmental entity. The recreation software scenario involves only the sharing of "personal information," and does not involve the sharing of PII. Moreover, even if the contract involved the sharing of PII, it's uncertain whether the software vendor would meet the third-party service provider definition because the vendor contracts with another entity to maintain and store data uploaded into the software and does not have an apparent obligation to process the data.
iv. C.R.S. §§ 24-85-101 through -104 and 24-34-802.
v. Promulgated by the Colorado Office of Information Technology (OIT) pursuant to C.R.S. § 24-85-103, including compliance with WCAG 2.1 AA Guidelines.
vi. "High-risk artificial intelligence system" means any artificial intelligence system that, when deployed, makes, or is a substantial factor in making, a consequential decision. C.R.S. § 6-1-1701(9)(a).
vii. "Consequential decision" means a decision that has a material legal or similarly significant effect on the provision or denial to any consumer of, or the cost or terms of: (a) Education enrollment or an education opportunity; (b) Employment or an employment opportunity; (c) A financial or lending service; (d) An essential government service; (e) Health-care services; (f) Housing; (g) Insurance; or (h) A legal service." C.R.S. § 6-1-1701(3).
viii. See C.R.S. § 6-1-1701(9)(b) ("high-risk artificial intelligence system" does not include systems intended to perform narrow procedural tasks).

Publication Date: 3/06/2025