Privacy and Data Security Vendor Contract Negotiation Guide

By May Tal Gongolevsky and Anthony Valanch, BakerHostetler

When entering into a contract with a vendor, most organizations focus on the services to be provided, and not data security. Although many of the vendor's services require access your data, contracts oftentimes do not clearly define the responsibilities and obligations of the vendor when doing so. With clearly defined privacy and data security provisions in vendor contracts, your organization can ensure that vendors have a responsibility to protect your data and there is an adequate remedy if they fail to honor that duty. Also, discussing these provisions during contract negotiations may provide valuable insight on the maturity of a vendor's information security posture.

Unfortunately, it is difficult, if not impossible, to apply the same privacy and data security provisions to every contract. It is important for your organization to determine the types of data to be accessed by the vendor, and what they will be doing with it. The answers to those questions will determine what provisions are necessary and how far you can "bend" before looking elsewhere. This guide will discuss certain privacy and data security provisions for your organization to consider when negotiating contracts with vendors that access or process your data.

1. Essential Privacy and Security Terms

Every contract with privacy and data security considerations will contain certain defined terms. Organizations should push for definitions that align with the business objectives of the contract and encompass all data accessed or processed by the vendor.

a. Personal Information – Properly defining this term will ensure the vendor's duties align with the organization's obligation to protect personal information under state and federal law.

- **i.** Require a clear, but broad, definition that protects a wide variety of information designated as confidential regardless of form or medium.
- **ii.** Review applicable state and federal privacy laws and regulations to and ensure that the information you are required to protect is included in the definition.
- **iii.** Draft definition to encompass all data points required by state data breach notification laws based on the residency of each data subject.
- **iv.** Consider all data sources the vendor may access while performing its duties, not just data within the scope of the engagement.
- **v.** If a vendor accesses or processes any personal information, such as personally identifiable information ("PII"), protected health information ("PHI"), or payment card information ("PCI"), include these items in the definition to ensure it is specifically protected.

2. **Confidentiality**

Contract language is often too narrow and omits provisions of confidentiality for information that is actually protected under state and federal law which can result in disputes if it unclear whether information that has been breached falls under the contract. Specifically we recommend that you think through the following:

- **i.** Make sure that the definition of Confidential Information is broad and applies to the relevant IP and data that the vendor collects; the lack of a comprehensive definition would increase the risk of disputes as to what is covered by the term. If the vendor collects any personal information, such as personally identifiable information ("PII"), protected health information ("PHI"), or credit card information, include these items in the definition of confidential information to ensure confidential treatment of the same.
- **ii.** If your organization is providing credentials to the vendor to access your network or systems, make sure that such credentials are considered confidential information.
- **iii.** Require access to confidential information only on a "need to know" basis.
- **iv.** Require vendor to enter into similar confidentiality agreements with staff, third-parties, and subcontractors who may have access to confidential information.
- **v.** Make sure that any customary exceptions to the duty to maintain confidence makes sense under your specific circumstances.
- **vi.** Make sure that any mutual confidential undertakings on your behalf do not affect your abilities to conduct certain business activities.

3. **Data Protection Provisions**

Clear and specific data protection provisions will allow your organization to limit its exposure due to a vendor's failure to employ standard security practices. Oftentimes, the data security measures a vendor agrees to in writing are not employed in practice. Organizations should consider establishing a certain set of standards to ensure the vendor's obligations align with your organization's data protection requirements. The data protection provisions should apply to all vendor personnel, including contractors and subcontractors with access to data. Depending on the relationship, you may want to require that all vendor personnel agree to the data protection provisions in writing.

- **a. Standard of Care** – It is important to establish a baseline standard of care for vendors to employ when accessing or processing your organization's information. Minimally, vendors should be expected to use the same degree of care, but no less than a reasonable degree of care, to prevent the unauthorized use, dissemination, or publication of your information as it uses to protects its own, including standard anti-virus/malware deployment.
- **b. Information Security Program –** Consider requiring your vendor to have a written information security program in place.
    - **i.** Decide on the required standards the vendor must meet depending on the information the vendor accesses or processes

ii. If applicable, vendor must comply with your internal privacy and/or information security policies.
iii. Think about establishing a set of information security standards for smaller vendors, or those who do not access or process PHI or PCI, and take into account the business relationship and maturity of the information security posture of the vendor.
iv. Consider requiring vendors of all sizes to conduct periodic penetration testing and/or risk assessments.

c. **Notification of an Information Security Incident** – In the event of an information security incident involving a vendor, timing is critical. Vendors will often try to conceal an incident fearing that it may lead to the loss of your organization's business. Requiring vendors to notify you of an incident will either give you the notice you need to address the situation, or provide a remedy in the event of a vendor's beach of this obligation.
    i. Consider requiring the vendor to notify your organization of actual or suspected use, disclosure, or acquisition of your data by an unauthorized actor.
        1. The vendor may attempt to limit notice obligation only to "actual" incidents. In such instances, you should assess the risk based on the services provided to determine if this is acceptable.
    ii. Immediate notification is preferred, 24-48 hours is acceptable.
    iii. Company may insist on reviewing/approving all vendor filings, communications, notices, or press releases related to an actual or suspected incident.
d. **Incident-Related Costs** – In the event that an incident occurred due to a failure of the vendor to secure your organization's data, consider shifting your costs associated with investigating, addressing, and responding to an incident to the vendor. The threat of exposure to these costs may provide the vendor additional incentive to keep your data secure.
e. **Vendor Personnel Screening/Training** – Due to the nature of your relationship with your vendor, your organization's control over who the vendor hires to provide services is limited. You may consider requiring that the vendor screen individuals who access or process your data for suitability and competence to ensure proper handling of sensitive data.
    i. Consider requiring criminal background checks and immediate termination of credentials for individuals who no longer need access to your organization's data.
    ii. Depending on the engagement, consider requiring the vendor to provide cybersecurity awareness and anti-phishing training to its employees.

4. Compliance with Privacy Laws

It may be helpful to set out the privacy laws that your organization expects its vendors to comply with. You should base the list of laws on the list you created using Module 2; however, here are some laws to consider depending on your industry and states where your data subjects reside:

i. GLBA (financial), FCRA (consumer reports / HR data), CAN-SPAM (marketing)
ii. PCI DSS – if handling credit card data
iii. Certain states impose minimum security requirements (e.g. California, Massachusetts, and New York

5. **Access to Systems**

The principle of least privilege – only permitting a user to access data that is necessary to perform their duties – is an important data risk management tool for organizations of all sizes. This principle can also be applied to vendors to help limit your exposure in the event of a data security incident. Your organization should also consider defining where your data can be stored and what happens after the vendor no longer needs access. Limiting who can access your data, and the available versions, can go a long way toward limiting the potential misuse of your data.

- **a. Restrictions** – Depending on the scope of engagement, you may consider the following restrictions for vendors who access or process your data:
  - **i.** Domestic Operations: No access or transfer of data to/from outside of the United States (domestic operations); international operations should be subject to the appropriate legal instrument(s) governing access or transfer.
  - **ii.** No modifications to company data.
  - **iii.** No unauthorized access.
  - **iv.** Restrict access to those who "need to know" in order to perform services under the agreement.
  - **v.** Require vendors to terminate credentials of an employee who no longer needs access to your systems to perform their duties. Credential management is a best practice to help limit activity by disgruntled individuals or malicious actors.
- **b. Data Storage** – Limiting the data that can be stored outside on your enterprise is an important data loss prevention tool. If data is contained in your environment, it is easier to control and protect. Consider the following data storage restrictions to prevent data from unnecessarily leaving your network:
  - **i.** Limit the data that can be stored outside of your environment to that necessary for a vendor to perform services and authorized by your organization.
  - **ii.** Do not permit the storage of company data on vendor mobile/removable devices (e.g. laptops, USB drives, or removable) except for limited purpose and duration.
- **c. Data Destruction** – By limiting the amount of data that may be compromised by malicious activity or mistake, an organization can significantly reduce its risk profile. Consider requiring that vendors to destroy or securely return your data upon termination or expiration of the engagement.

6. **Audit Rights**

Trust, but verify. Agreeing to certain information security measures and standards is one thing, enacting and enforcing them is another. Consider requiring vendors to submit to information security audits or questionnaires to ensure compliance with the requirements of the agreement. Below are a few audit considerations for your organization when negotiating vendor contracts.

- **a.** Determine who will conduct the audit – vendor, third-party, or resources at your organization.
- **b.** Decide on the scope and frequency of the audit as determined by the size and information accessed by the vendor.

i. The less onerous the audit measure, the more frequently it can be requested.
    1. Penetration testing – monthly
    2. Risk Assessments – quarterly
    3. Full SOC 2, Type II, or ISO 27001 certification – yearly

For details on topics to cover in as part of the audit please refer to the Compliance Audit Guide included in this module.

7. Indemnification and Limitation of Liability

Most vendor contracts contain inadequate liability and indemnification provisions in connection with data breaches. Standard limitations on liability are most likely too low to cover the costs related to a breach as breaches often expose companies to significantly high costs for remediation and legal fees. If the vendor had more control over the factors giving rise to a particular risk, the vendor should bear more responsibility in the event that such risk materializes and results in damages to your company. Vendors often limit liability, disclaim consequential damages, and impose a low general liability cap. To evaluate whether these limitations are reasonable, you need to evaluate the risk that vendor's nonperformance or misconduct may require you to spend additional funds to address problems you did not create and beyond your control.

a. **Security breaches** – Push liability for security breaches and failure to timely notify thereof to vendor; indemnity should cover any breach of confidentiality and security obligations. You should not only require that the vendor indemnify you, but also that the vendor cooperate with any pending litigation or investigation in connection with security incident.
b. **Carve-outs:**
    i. Insist on exceptions to a limitation of liability cap in instances of gross negligence, willful misconduct, or fraud and in cases of third-party claims.
    ii. Limitation of liability provisions should not disclaim the costs of termination and any additional costs you may incur to obtain alternative functionality as promised in the original contract that vendor failed to deliver.
    iii. Exclude breach of confidentiality, data security, notification and data privacy obligations from the limitation of liability provision to the greatest extent possible. If vendor will not exclude such claims, attempt to negotiate a separate liability cap.
c. **Remedies** – Limitation of liability provisions should address specific remedies in the event of a breach, including liquidated damages, the right to seek injunctive relief, the right to terminate, credit for not meeting service levels, the release of materials from escrow, breach notification reimbursement, special damages for epidemic failure, etc.
d. **Impact on Insurance** – If you agree to indemnify vendor against third-party claims, consult with your insurance broker to make sure your policy covers the claims and to understand the potential impact of such indemnification language on coverage in general.
e. **Autorenewal** – If the agreement renews automatically, reserve the right to review and renegotiate liability and indemnification provisions to ensure that these adequately protect against new cybersecurity threats and related financial consequences.

8. **Warranties**

Generally, vendors tend to disclaim all warranties unless specifically stated otherwise. It is therefore crucial to include affirmative, express warranties regarding security. Warranties should be tailored to match the specific services rendered.

- **a.** Require vendor to provide warranties of adequate internal security standards and any such standard that specifically relate to the product acquired or services rendered.
- **b.** Require vendor to give ample prior notice of any material changes to the deliverables that could adversely affect security and/or data integrity.
- **c.** Vendor should represent that any work product should be free and clear of viruses.
- **d.** Vendor should provide proper documentation and/or user manuals describing the deliverable and technical specifications. Work product and all related equipment, software and systems should substantially conform with such documentation.
- **e.** Make sure that the exact period of vendor warranty against defects is conspicuously stated in the contract.

9. **Termination**

The ability to terminate an agreement with a vendor who did not adhere to certain security standards or suffered a breach is essential to the protection of your data. Even if a breach was not involved, the termination of a contract may present additional risk to your company because the vendor may no longer be under any duty to protect your confidential information. Consider the following to award your data maximum protection and to transition the engagement to another provider swiftly and effectively:

- **a. Termination due to a security failure** – If termination for convenience cannot be agreed upon, reserve the right to terminate if vendor fails to comply with its security representations and obligations under the agreement (those do not have to amount to a full-blown breach).
- **b. Return of materials upon termination** – Vendor should return or destroy all data and materials provided to vendor or created by vendor in the course of the engagement. Sever access to any systems post-termination should be provided for.
- **c. Transition Assistance** – Require assistance if data or materials need to be transferred to a subsequent service provider.
- **d. No data "Lockout"** – Vendor should return data and materials regardless of any other open items and payment obligations; data should not be held "hostage."

10. **Subcontractors and liability for third parties**

When engaging a vendor who may use subcontractors to provide the contracted services, your main objective is to hold the vendor to the same performance standards and liabilities regardless of who performs the work. Therefore, the vendor should require any subcontractors to meet the same security standards as vendor is required to meet. Key considerations include the following:

- **a.** Vendor should ensure that any of its subcontractors adhere to the same security levels standards as the hiring vendor.

b. Vendor should be accountable and liable for any acts or omissions by third- parties (such as failure to employ adequate security measures) in accordance with any limitation of liabilities/indemnification provisions in the contract.

c. **Permission to Subcontract** – Vendor should seek prior authorization to subcontract in writing. If vendor will not agree to prior written consent, vendor should at a minimum promptly notify you of any subcontracting. Vendor should not be permitted to subcontract services that access or process sensitive company information.

d. **Access** - Make sure that third-party access rights are spelled out conspicuously to help control who has access to the data and how it can be used when multiple participants are involved.

11. Preservation Notices and E-Discovery

Records, documents and communications with the vendor may become relevant if litigation is brought against your company due to a security incident. Consider adding language along the lines of the following to ensure in advance that the vendor complies with discovery requests to help avoid friction over this issue in the future.

a. It is beneficial to add language ensuring vendor's compliance with a third- party legal hold notice in the event of litigation, any preservation notices and document requests.

b. In instances where the vendor provides software/platform, vendor should allow you to retain an archival copy of the most recently used version of the software and all documentation in the event that discovery requests call for electronically stored information in native format.

12. Insurance

The contract should include language that the vendor will carry sufficient cyber risk or other insurance to cover damages resulting from an information security incident. Make sure that your company is an additional insured and request a certificate of insurance annually.

May Tal Gongolevsky is a partner in the New York office of BakerHostetler. She counsels clients on issues relating to electronic discovery, data privacy, software licensing, and general law and technology issues. As an attorney with a technical background as a computer programmer, she understands, advises and counsels clients on a myriad of legal and technical questions relating to the electronic discovery process, data mapping and technology licensing.

Anthony Valach is a counsel in Privacy and Data Protection practice at Baker Hostetler, in the Philadelphia office.