LEWIS BRISBOIS BISGAARD & SMITH LLP
ATTORNEYS

# Information Security Best Practices

## Service Provider Agreements

LewisBrisbois.com

# Information Security Best Practices: Service Provider Agreements

*A business retains a vendor to perform customer-billing services. One of the vendor's computers is hacked from an IP address in China when a server is inadvertently left without a firewall following an internet outage. The attack compromises customer credit card information, and triggers notifications statutes throughout the country. As between the business and the vendor, how will responsibility for responding to the event handled? The answer may lie in a thoughtfully drafted service provider agreement.*

Events like this hypothetical situation occur with increasing frequency, illustrating the risk vendors may represent to data security. Virtually every enterprise handles the personally identifiable information (PII) of its employees, clients or customers. This information is frequently made accessible to vendors and service providers for a variety of reasons. While this sharing of information may be a necessity, it can increase the risk of unauthorized disclosure of PII. A data privacy event exposing PII will cause financial harm and may damage an entity's reputation. As the number of data privacy events continues to rise, entities are well advised to anticipate privacy exposures when negotiating service provider agreements (or vendor agreements). This paper addresses best practices to minimize risk associated with PII when entering into such agreements. For further assistance, the Appendix provides a general checklist for use in drafting, reviewing and negotiating vendor agreements.

## Know Your Service Providers

Before signing a service provider agreement, an entity should determine the following (at a minimum):

- If the relationship will involve the service provider's access to PII;
- What types of PII are involved;
- Does the service provider have written data privacy and security policies;
- Does the service provider enforce and audit compliance with those policies;
- Does the service provider have adequate data privacy insurance coverage;
- Does the service provider restrict access to PII;
- How will the PII be managed by the service provider;
- How, if at all, does the service provider screen employees who will access PII;
- Does the service provider have a written incident response plan in the event of a data privacy event?

The service provider's answers to questions like these will assist an entity in addressing the risk to the PII in the service provider agreement.

Do not overlook a fundamental focus on due diligence. Evaluate the service provider's potential involvement in past data privacy incidents. Assessing a service provider's past experience is equally as important as assessing your own current risks. Significant past incidents may have received media attention, or be listed on the websites of state attorneys general. A web search can yield meaningful privacy history about a service provider and highlight red flags, such as a service provider that has repeatedly mismanaged data privacy issues.

## Get It in Writing: Service Provider Agreement Terms and Conditions

Purchase orders are simply not sufficient to properly establish clear privacy and security duties between contracting parties. An entity should incorporate basic data privacy and information security terms and conditions in service provider agreements. Below is a discussion of some of the specific clauses that should be addressed.

### 1. Addressing A Data Privacy Event in the Service Provider Agreement

An entity should request the right to periodically audit its service provider's data privacy policies, procedures and employee training to ensure compliance. The service provider agreement should include language setting expectations regarding when, how and under what circumstances a service provider will report potential or suspected data compromises. An entity should request the right to investigate any incident involving its PII, including the right to obtain third party confirmation of the scope of the possible compromise. For example, the service provider agreement should set forth that the service provider must: 1) notify the entity immediately after discovery of a potential or suspected compromise of PII, and 2) provide specific details, such as the who, what, when, where, and how of the event. As investigations into data privacy events unfold, new details will emerge. The service provider agreement should provide for regular updates from the service provider.

Consider language outlining the service provider's immediate duties upon the discovery of a possible data event requiring the service provider to:

- Report promptly upon determination that a potential or suspected data compromise has occurred;
- Provide access necessary to enable the entity to obtain its own evaluation of the facts;
- Cooperate to the fullest extent with any forensics investigation conducted by a third party;
- Grant the entity the right to control the breach response, including selection of response vendors;

- Remedy immediately the cause of the compromise at service provider's sole expense; and

- Preserve all paper and electronic documentation related to the event.

### 2. Contractual Indemnification

Indemnification clauses allow a contracting party to shift liability and defense exposure to another. It is important for an entity to thoroughly analyze indemnification provisions in a service provider agreement to ensure that the entity is not inadvertently agreeing to bear the costs of a data privacy incident caused by its service provider, or agreeing to defend and indemnify its service provider against third party claims. On the other hand, the entity should request as much affirmative protection as possible against third party lawsuits and first party costs by inserting an indemnification provision of its own that requires the service provider to absorb the entity's liability exposure, defense, and crisis management costs.

Indemnification language may include that:

- Service provider should indemnify, defend, and hold harmless the entity from all claims, allegations, causes of action, or demands that are presented to service provider by a third party (including any contractor);

- After a suspected data compromise, the service provider should indemnify the entity's losses, liabilities, damages, lost premium, fines, penalties, assessments and related costs and expenses including crisis management costs (such as legal, forensics, public relations, notifications, call center, and identity protection services), reasonable costs of litigation, court costs, attorneys' fees and interest.

### 3. Limitations of Liability

Limitation of liability clauses set forth terms limiting legal liability, such as shortening the amount of time within which claims may be brought by one party against the other, setting a monetary limit on damages, or limiting the types of damages a party may recover. An entity should avoid any limitation on damages that prevents it from recovering the first and/or third party costs of a data privacy incident if the service provider is responsible for the data privacy event.

In an actual negotiation, it should be anticipated that the service provider will take the opposing position concerning limitations of liability. An entity should resist limitations of liability clauses that render the service provider liable only if the service provider's sole negligence or willful action is the cause of the event, or if the clause shortens the statutory time the entity otherwise would have to make a claim. As each situation is different, it will be up to the entity to ultimately determine the importance of a limitation of liability for itself versus the value of not limiting its service provider's liability when a data privacy

event occurs. Factors will include the extent to which the service provider will have access to PII, the strength of the vendor's own security as revealed in a due diligence investigation, the importance of the service provider to the entity's core functions and similar considerations.

### 4. Leverage a Service Provider's Insurance Coverage

An entity should require its service provider to produce proof of data privacy insurance that will cover the first and third party costs incurred because of a data privacy event. The service provider's carrier, not the broker, should issue this proof or certification. A service provider may not realize that its Commercial General Liability policy does not provide coverage for many (or any) of the costs, particularly the first party costs, associated with a data privacy event. The service provider agreement should require that the entity be named as an additional named insured on the service provider's data security policy, and that the service provider's insurance policy be designated as the primary policy in the event of a data privacy event. The entity should obtain yearly confirmation by, at minimum, a current declarations page showing the entity as the additional named insured and best case, a certified copy of the entire policy for the entity's records.

### 5. Warranty Clauses

Warranty clauses provide assurances that goods and services will perform or be conducted a certain way, and/or in compliance with applicable laws and regulations. Often, service providers will attempt to include language limiting express warranties for their goods or services, and/or implied warranties provided by law, such as the implied warranties of fitness for a particular purpose, merchantability, or performance of services in a competent manner. While these clauses are common, entities should analyze these warranties to determine how these clauses may affect data privacy concerns. Such language may purport to apply to not only the service provider, but also to any subcontractors hired by the service provider who may be completely unknown to the entity.

Service providers may outsource a portion of their services to subcontractors who have access to the entity's PII. As a best practice, an entity should require that the service provider warrant that any hired subcontractor who has access to the entity's PII will not only be qualified (and appropriately insured) to perform services, but also that the subcontractor will abide by the service provider's privacy policies and the other terms in the service provider agreement related to data privacy events. Warranty clauses may provide that the service provider will obtain a signed agreement from the subcontractor to comply with all privacy policies and protocols set forth in the service provider agreement.

### 6. Amendments

A service provider may attempt to incorporate language into the service provider agreement that allows it to freely amend the service provider agreement's terms at any time to accommodate technological updates that may affect service. An entity should pay special attention to provisions providing for amendments, and pay attention to the amendments themselves, to prevent the service provider from unilaterally changing its substantive privacy practices and duties. If possible, the entity should avoid language permitting unilateral changes in the service provider agreement.

### 7. Waivers of Subrogation

A waiver of subrogation clause prevents a contracting party's insurance carrier from seeking compensation from another contracting party (and usually its subcontractors). Waivers of subrogation usually apply even if the party benefiting from the waiver was negligent in the performance of its contractual duties. Courts frequently uphold waivers of subrogation even when insurance carriers are unaware of their inclusion in contracts. If a waiver of subrogation is contained in the service provider agreement, an entity may have waived its recovery rights (or its carrier's rights) against a responsible party. Therefore, entities should make every effort to eliminate these waivers.

### 8. Choice of Law Provisions

Choice of law provisions dictate the state's law that will govern a dispute related to or arising under the service provider agreement, and the venue in which such dispute will be litigated. Choice of law provisions are often included in service provider agreements. Preemptive analysis of the jurisprudence surrounding the contractual issues discussed throughout this document should be performed to determine the most favorable jurisdiction should a data privacy incident occur. This can be especially important if the service provider is not located within the United States. Suggested best practices for a choice of law provision include that the parties agree to be governed by the law of a specific state within the United States and make the courts of that state the proper venue for lawsuits.

### 9. Special Considerations When Using Cloud Service Providers

Use of a cloud provider allows an entity to avoid the bulk of the cost of infrastructure and IT services necessary to manage data. Use of the cloud presents its own set of challenges. Recognizing the inherent unequal bargaining power of the entity when dealing with some cloud providers, an entity should ensure that data in the cloud is properly protected and stored, and that access to the information is limited to appropriate individuals. The nature of the cloud means that data will almost certainly travel across state lines, if not internationally, so special attention should be paid to choice of law issues. At a minimum, service provider agreements with cloud providers should provide that: 1) the infrastructure housing the entity's data will remain in the United States, 2) that the

cloud service provider will report potential or suspected data events as discussed above, and 3) that the cloud service provider will agree to allow access to its infrastructure for forensic investigations of data events. The service provider agreement should provide concrete terms in the event of the termination of the service provider agreement to ensure that data will be properly transitioned out of the cloud.

## Conclusion

This paper illustrates a non-exhaustive variety of concerns that should be addressed by an entity when creating a service provider agreement. When negotiating service provider agreements, entities can anticipate that service providers will take the opposite positions on these issues. An entity serving in the role of a service provider may itself want to take the opposite positions on the issues discussed. Each situation will pose its own unique circumstances and challenges depending on a number of variables, including the bargaining power of the parties. Essential risk management opportunities should be considered during service provider agreement negotiations. To protect PII and ensure the service provider takes appropriate steps in response to data privacy events, areas of potential concern in service provider agreements go beyond typical terms regarding price and scope of services. Entities should be cognizant of the issues discussed in this paper whenever entering into any service provider agreement where the vendor may have access to PII.

## Appendix – Checklist for Negotiating, Drafting and Reviewing Service Provider Agreements

The following checklist provides a summary of key privacy issues an entity should consider when entering into service provider agreements. While the list is by no means exhaustive, addressing these issues will lend clarity to the risks presented. For specific questions, it is recommended that you consult an attorney.

Take a look at a recently prepared agreement and recall the process followed to develop that agreement. You can score your company's readiness regarding the processes and contract provisions listed below. Each question is assigned a value. As you read the questions on the list, if your answer is yes, write the number on the line next to the item. Tally your numbers to get your score. The chart at the end of the list will explain what your score means.

| **Know Your Service Provider** | **Item Value** | **Your Score** |
|---|---|---|
| • Do you perform due diligence on the service provider, including checking references, asking questions related to PII handling, and researching the service provider on the Internet? | 20 | _____ |
| • Do you examine the service provider's data privacy policies and incident response plan? | 10 | _____ |
| **Get It in Writing: Service Provider Agreement Terms and Conditions** | | _____ |
| • Do you define basic data privacy and information security terms and conditions in writing? | 20 | _____ |
| **Addressing a Data Privacy Event in the Service Provider Agreement** | 20 | _____ |
| • In the event of a potential or suspected data privacy event, do you require prompt notice, investigational cooperation, and assurance of remediation of the data exposure? | 20 | _____ |
| **TOTAL PAGE 1** | **90** | _____ |

| **Contractual Indemnification** | **Item Value** | **Your Score** |
|---|---|---|
| • Do you eliminate or modify indemnification clauses that shift costs of a data privacy event away from the service provider and on to the entity? | 20 | _____ |
| • Do you seek indemnification for data privacy events caused in whole or in part by the service provider and/or a third party? | 25 | _____ |
| **Limitations of Liability** | | |
| • Do you limit the entity's liability to the service provider for data privacy events? | 15 | _____ |
| • Do you eliminate limitation of liability clauses that shorten the time for an entity to bring a claim? | 15 | _____ |
| **Warranties** | | |
| • Do you require the service provider to warrant that employees and subcontractors will access PII only when necessary and will abide by the terms of the service provider agreement and any related privacy policies? | 20 | _____ |
| **Amendments** | | |
| • Do you eliminate language that allows the service provider to unilaterally amend language in the service provider agreement? | 20 | _____ |
| **Waivers of Subrogation** | | |
| • Do you eliminate waivers of subrogation? | 15 | _____ |
| **Choice of Law Provisions** | | |
| • Do you include a choice of law provision that selects which U.S. state's law governs and which court is the proper venue for any litigation? | 15 | _____ |
| **TOTAL PAGE 2** | **145** | _____ |

| Contractual Indemnification | Item Value | Your Score |
|---|---|---|
| • If dealing with a cloud provider, do you require terms that provide for protection, storage, and location of data? | 20 | _____ |
| • Do you ensure that data will be properly transitioned out of the cloud following termination of the service provider relationship, and address the future handling, return, or destruction of PII in service provider's possession? | 20 | _____ |
| **TOTAL PAGE 3** | **40** | _____ |
| **TOTALS PAGES 1, 2 AND 3** | **255** | _____ |

**What Your Score Means**

Whatever your score, you should always consult an attorney to determine the legal and practical significance of contract provisions. The above self-assessment and this analysis are to assist you when discussing these issues with your attorney. Any one item above for which your score is 0 could create an issue leading to liability, and a perfect score is not a guarantee that you are fully protected.

**If your score is between 230 and 255:**
Your process and contract terms are strong permitting reasonable protection of data and the ability to better address data security incidents should they arise.

**If your score is between 200 and 225:**
Your process and contract terms are good, but there are areas that should be addressed to permit reasonable protection of data and the ability to address data security incidents.

**If your score is between 175 and 195:**
Your process and contract terms are fair, but a reassessment of all contracts and contracting processes is recommended.

**If your score is below 175:**
Contract processes and terms should be discussed with your attorney.