How to Negotiate Data Security Addendums with Confidence

Technology, Privacy, and eCommerce

CHEAT SHEET

- ***Explain it.*** Convey — fast and thoroughly — to the procurement department what specific type of data will be involved in a data security addendum.
- ***Agree to terms.*** Defining “personal information” is key to determining each party’s rights and obligations within the data security addendum, so carefully construct the definition to prevent any improprieties.
- ***No international conflict.*** If the vendor’s services transfer data from the European Union to the United States, refer to the EU Commission model contracts for guidance.
- ***Tech support.*** Data security addendums should also include provisions requiring certain data backup procedures, data recovery plans, encryption standards, and other technical safeguards.

A vendor sitting across the table from a prospective multinational client is faced with significant challenges in trying to win the contract. It can be a daunting task to perform services for a multinational corporation with a presence in Asia, Africa, Europe, and the Americas. Among other things, multinational companies often have sophisticated, multi-step vendor management programs. To a smaller vendor, that can mean there is no clear indication as to when (or if) a deal will be inked.

> It is also important to remember that the statutory or regulatory definition of “personal information” may be different depending upon the jurisdiction from where the data originates, the country in which the vendor is based, or the country in which the multinational will be

using the data.

So, what is a vendor to do when it feels like David facing Goliath? This article provides some suggestions on how to help expedite complex reviews prompted by vendor management programs, and to understand some of the contracting issues that are likely to arise when you are presented with a “template” data security or data privacy addendum by a multinational prospect.

Educate your client’s procurement department

It’s important to understand some of the internal drawbacks in the contracting process for multinational companies. Among other things, realize that the plethora of contracting steps that may be thrown at a vendor (from security questionnaires to security and privacy addenda) are often driven by the fact that a contracting or procurement department may not understand what the service provider intends to do for the company. Put differently, while the business may be interested in a service provider’s product, and understand its function and purpose, that knowledge is often not well conveyed to the procurement department that is expected to on-board the vendor. For example, some procurement departments may use the same vendor questionnaire for an operator of a cloud platform and for a company that solely provides implementation and maintenance services for a customer’s cloud platform. Procurement departments sometimes respond to this lack of information by throwing “everything including the kitchen sink” at a vendor to make sure that their bases are covered.

Therefore, one of the service provider’s first tasks is to help a prospect’s procurement department understand — quickly and efficiently — what type of data will be involved so that they can (hopefully) adjust the contracting process for the risk level. Among other things, this means being prepared to answer basic questions for the procurement department — or better yet volunteer this information before being asked:

- What specific service is being requested of the service provider?
- Will the service provider be using third-party contractors to perform the services (e.g., subprocessors)?
- Will any personally identifiable information be transferred to the service provider?
- If so, will any of that data be of higher sensitivity such as financial information, credit card information, medical records, Social Security Numbers, or biometric records?
- Is the service provider (or the company) subject to specific regulatory rules or guidance with respect to the data that will be transferred (e.g., HIPAA, PCIDSS, FERPA, etc.)
- From what country/countries will the data originate, and to what countries will the data be transmitted?

Definition of personal information

The definition of “personal information” is often critical in determining each party’s rights and obligations under the data security addendum. It is important for both parties to carefully craft the definition of personal information. Too broad of a definition could include the name and email address of the businessperson corresponding with the service provider and may put unreasonable burdens on protecting, storing, and processing such information. Too narrow a definition could exclude types of personal information subject to laws that require certain protective contract provisions.

Depending on what kind of personal information is being handled, it is important to make sure that the definition lines up with the restriction requirements in the addendum. It is also important to remember that the statutory or regulatory definition of “personal information” may be different depending upon the jurisdiction from where the data originates, the country in which the vendor is based, or the country in which the multinational will be using the data. While on some level you may want your contractual definition of “personal information” to align with statutory definition of the term, at other times the term may be used in your contract in ways that are beyond the scope of the related statutes. The net result is that adopting a statutory definition often makes a contract either too broad or too narrow. For example, if a contract will involve the processing of data under the EU General Data Protection Regulation (GDPR) you might be tempted to adopt the GDPR’s extremely broad definition of “personal data” as any data that relates, or could relate to, an individual. If you were to adopt that definition as the primary reference point in a contract you could, however, end up imposing security or privacy restrictions on data that is not subject to the GDPR, or on data that is not even part of the service.

One way to account for the different treatment of various levels of personal information is to create separate personal information categories with different levels of sensitivity. A category such as “contact information” could be used for names, addresses, and email addresses and include requirements to encrypt such information only while in transit. Whereas, a “sensitive data” category may include social security numbers, credit card information, and national identifiers. Restrictions for the service provider with regard to this category could include specific types of encryption standards to be applied while the data is at rest and while it is in transit.

Defining a breach and notification requirements

Many data security addendums require that a service provider notify a customer anytime it suspects that its customer’s personal data may have been involved in a security incident. This obligation often stems from US state or other data breach notification requirements that may trigger notification of governmental entities or data subjects following a “data breach.” If the notification provision is vague or overly broad, there is a risk that the language will, on its face, require the service provider to disclose any possible exposure or access to the customer’s personal data. From a practical standpoint, systems are threatened frequently and service providers can be the target of multiple “security incidents” on a daily basis. These threats can include phishing emails or users being locked out of their user accounts.

To avoid providing notice for incidents that likely have no impact on a customer’s data, consider including a materiality definition to limit the scope of “a security incident.” Questions to ask include: (1) Will this definition include any breach of the service provider’s systems? (2) Would the breach be a threat or compromise the company’s data? Also consider whether a client wants to be notified of every suspected security incident. In certain regulatory regimes — such as Europe’s GDPR — once the service provider has provided notice to a customer of a possible security incident it puts the customer in the position of having to make a determination as to whether the possibility of the security incident is sufficient enough to trigger a 72-hour clock in which regulators might have to be notified. In retrospect, many companies have wished that their service providers were more judicious in informing them (or not informing them) of security incidents that have a low probability of harm (or even occurrence) and that the service provider had, instead, conducted a basic investigation before providing notice.

Vaguely drafted breach notification provisions are those that include broad language that requires reporting for any incident that “could” or “may” put customer data at risk. Due to the fact that in

many instances it is difficult to determine whether an incident could put customer data at risk, it is important for the service provider to suggest qualifiers that limit the definition of a breach to an unauthorized acquisition or loss of personal information that is reasonably likely to put customer data at risk. Negotiating this provision could include a lot of back and forth and, therefore, a mutual compromise between the parties may be to mirror the data breach notification statute of the jurisdiction in which the company operates.

Does not conflict with EU model contract clauses

If the services provided by the vendor relate to the transfer of data from the European Union to the United States, there may be international data transfer issues that are not contemplated during a strictly in-country data transfer. The EU Commission has created model contracts to facilitate the transfer of personal information from Europe to the United States (also known as “model clauses”) and has determined that organizations that use the model clauses offer sufficient safeguards for cross-border data transfer as required by the GDPR. In order to be deemed effective for cross-border data transfer, model clauses cannot be modified and cannot conflict with any other contractual provision between the parties. Both parties should verify that the model clauses do not conflict with the data security or data privacy addendum. In addition, it is important for both parties to take steps to ensure that the addendum and the MSA includes a provision that clarifies the model contracts hold priority above all other documents in the event of conflicting documents.

Compliance with international laws

One of the most common and problematic provisions in a data security addendum is a covenant and warrant that the service provider complies with “all applicable data privacy laws.” While this may seem inconspicuous and innocent, it could be nearly impossible for a service provider to comply with it. As mentioned earlier, stringent global restrictions exist in some European and Asian countries that regulate cross-border data flows. For example, if the company sends the service provider personal data from German citizens, but did not tell the service provider that the data relates to Germans, the service provider would be incapable of knowing that German data protection laws may apply to the information that it receives.

> If you hear the term “localization” in the context of personal information transfers, be aware that there may be a requirement to keep that data in the originating country and to have a redundant system in the receiving country.

Additional problems could arise if the company collects personal data about Russian citizens and needs to transfer it across international borders. For example, in 2014, Russia passed a law requiring an updated copy of Russian citizens’ personal data to be stored in IT systems or data centers in Russia. If you hear the term “localization” in the context of personal information transfers, be aware that there may be a requirement to keep that data in the originating country and to have a redundant system in the receiving country. Therefore, knowing where your service provider operates and the locations where the data is being transmitted are important facts to know during the vendor selection process.

One approach when including a “comply with all applicable law provision” is for the company to notify the service provider in the contract what information is being transmitted and what jurisdiction the information is from. At the same time, it is important for a service provider to disclose all

jurisdictions where they operate and in what locations they store and process the data.

Processor and service provider requirements

REQUIREMENT	GDPR	CCPA
PARTICULARS:		
1. Subject Matter. Description of the subject matter of processing.	✓ Art. 23(3)	✗
2. Duration. Description of the duration of processing.	✓ Art. 23(3)	✗
3. Nature and Purpose. Description of the nature and purpose of processing.	✓ Art. 23(3)	✗
4. Type of Data. Description of the type of personal data to be processed.	✓ Art. 23(3)	✗
5. Categories of Data. Description of the categories of data subjects about which the data relates.	✓ Art. 23(3)	✗
RESTRICTIONS		
6. Use Restrictions. A service provider can only process personal data consistent with a controller's documented instructions.	✓ Art. 28(3)(a)	✗
7. Disclosure Restrictions. Confidentiality provision that ensures that persons authorized to process personal data have committed themselves to confidentiality.	✓ Art. 28(3)(a)	✗
8. Delete or Return Data. Service provider will delete or return data at the end of the engagement.	✓ Art. 28(3)(a)	✗

SECURITY		
9. Security. Service provider will implement appropriate technical and organizational measures to secure information.	✓ Art. 28(1) Art. 28(3)(c) Art. 32(1)	✗ (although other California laws apply to data breach response)
10. Assisting Controller in Responding to Data Breach. Service provider will cooperate with controller in the event of a personal data breach.	✓ Art. 28(3)(f) Art. 33 – 34	✗
SUBPROCESSING		
11. Subcontractor Selection. A service provider must obtain written authorization before subcontracting and must inform the company before it makes any changes to its subcontractors.	✓ Art. 28(2) Art. 28(3)(d)	✗
12. Subcontracting Flow Down Obligations. Service provider will flow down these obligations to any subprocessors.	✓ Art. 28(3)(d) Art. 28(4)	✗
13. Subcontracting Liability. A service provider must remain fully liable to the controller for the performance of a sub-processors obligations.	✓ Art. 28(3)(d)	✗
DATA SUBJECT / CONSUMER REQUESTS		
14. Responding to Data Subjects. Service provider will assist the company to respond to any requests by a data subject.	✓ Art. 28(3)(e) Art. 12 – 23	✓ § 1798.105(c) (relating to deletion)
MISCELLANEOUS		
15. Assisting Controller In Creating DPIA. Service provider will cooperate with controller in the event the controller initiates a data protection impact assessment.	✓ Art. 28(3)(f) Art. 35) Art. 35-36	✗
16. Audit Right. Service provider will allow company to conduct audits or inspections for compliance to these obligations.	✓ Art. 28(3)(h).	✗
17. Cross-border Transfers. Service provider will not transfer data outside of the EEA without permission of company.	✓ Art. 28(3)(a) Art. 46	✗

Technical obligations

Data security addendums may include obligations that require certain data backup procedures, data recovery plans, encryption standards, and other technical safeguards. It is important to determine where the data originates to know what security standards may be required. Some countries' data protection laws (e.g., the United States, Spain, and Germany) include requirements that certain types of sensitive data be encrypted while in transit.

Security audit requirements

Some customers require that a service provider perform annual security audits by an independent third-party auditor. While this requirement is in itself not usually problematic, some companies require the service provider to provide all data security audits conducted of the service provider during the term of the MSA and to fix all reported security vulnerabilities. These requirements could pose two issues for the service provider. First, when a service provider conducts an audit, the report often includes a list of critical, as well as minor, security vulnerabilities. It is often impractical from a business perspective to fix all minor security vulnerabilities. The addendum might instead provide that critical or major security issues be remediated immediately and if not, the provision could allow the company to terminate the MSA without penalty.

> In the event of a security incident that involves an extraction of data, companies typically retain a forensic investigator, usually through outside counsel.

Second, requiring the service provider to provide all of its data security audits could waive the service provider's attorney-client privilege. In the event of a security incident that involves an extraction of data, companies typically retain a forensic investigator, usually through outside counsel. If the investigator's report were to be provided to a multinational company, it could affect a global waiver of privilege, resulting in third parties receiving the security report as well (e.g., plaintiffs, Visa/MC/AMEX, etc.). This could impact the service provider in any future litigation as well as expose information about the company to third parties. These types of unintended results need to be carefully considered prior to requiring that a service provider provide the company with results of all audits conducted during the MSA term.

Non-negotiable contracting terms

Smaller vendors that are not used to dealing with multinational companies sometimes do not realize that some of the contracting terms requested by a multinational client are simply nonnegotiable. For example, if data that will be received by the service provider is subject to Europe's GDPR, and the service provider will be considered a "processor" under that statute, Article 28 of the GDPR requires that the multinational "bind" the service provider to approximately 17 substantive provisions; it also requires that contracts with service providers contain specific disclosures concerning the type of processing that will be covered by the agreement. In comparison, if data that will be received by the service provider will be subject to the California Consumer Privacy Act (CCPA), and if the multinational needs the vendor to fall within the definition of "service provider" within that statute, the multinational may only need the contract to include four or five of those substantive provisions. Therefore, it's imperative to ascertain what contracting terms are mandated by the jurisdiction.

The chart on processor and service provider requirements compares the requirements that the

GDPR imposes on processors with those that a business should impose upon a service provider pursuant to the CCPA. As the chart indicates, whether the data that a vendor may be processing is subject to the GDPR or the CCPA makes a significant difference when it comes to which contractual provisions are functionally mandatory upon the vendor.

In today's world of massive data breaches and new privacy laws, every vendor's data security and privacy compliance will be scrutinized. Most medium and small companies that act as vendors to larger enterprises will need to negotiate a data security or privacy addendum that protects the vendor, but also delivers security to the enterprise. In order to be properly positioned for the contracting process, vendors need to carefully review data security and privacy requirements and evaluate their current practices to determine what they can and cannot accept.

ACC EXTRAS ON… Data security

ACC Docket

How to Reduce Your Cybersecurity Risk Profile through Vendor Management (Aug. 2017).

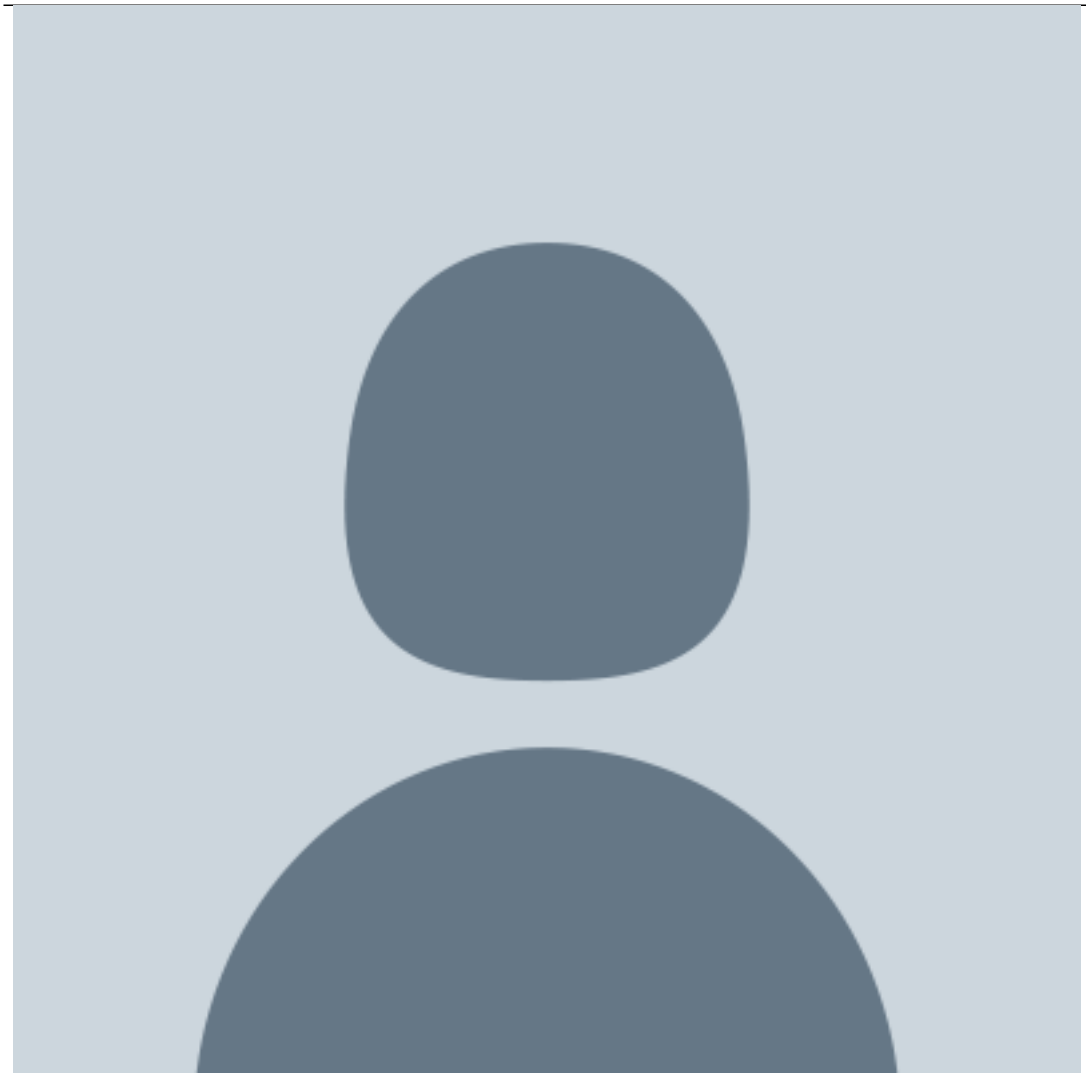
Standing Up for Data Protection and Personal Security (May 2017).

Practical Data Security Takeaways from Australia's Recent Privacy Determination (Feb. 2017).

Sample Forms, Policies, and Contracts

Privacy and Data Security Addendum (March 2017).

David Chen



Privacy Counsel

Unibail-Rodamco-Westfield

Unibail-Rodamco-Westfield is a commercial real estate company headquarted in Paris, France.

David Zetoony

Shareholder

Greenberg Traurig

David Zetoony, co-chair of the firm's US Data, Privacy, and Cybersecurity Practice, focuses on helping businesses navigate data privacy and cybersecurity laws from a practical standpoint. He is based on Denver, Colorado.