Be Careful about Personal Data Protection Clauses – Review Them Closely Before Agreeing to Them

Legal Alert
January 29, 2013

Garvey Schubert Barer Legal Update, January 2013.

Government contractors should agree to contract clauses for the protection of personal data – but be careful to make sure such clauses are fair, reasonable, and doable.

Many government contractors work on government IT projects that involve databases containing personal data of government personnel, employees of regulated entities, and perhaps the general public. The threat of security breaches and unauthorized disclosures of such personal data is causing many contractors to take risk mitigation measures, such as transferring as much risk and liability onto their subs as possible. In addition, a proposed new FAR clause will establish minimum data security requirements for federal contractors with access to government information. (See 67 Fed. Reg. 165 (Aug. 24, 2012) pp. 51496 – 51499.) As a result, many second- and lower- tiered contractors are now seeing contract clauses requiring them to adopt strict data protection measures and imposing on them serious penalties if such measures are breached. While data protection is a worthy goal, subcontractors, particularly small companies, must review such clauses carefully and avoid agreeing to overly strict or impossibly difficult obligations - and unreasonable penalties. In addition, such subs must adopt their own risk mitigation measures, such as adding cyber security insurance coverage. Otherwise, a subcontractor may find itself with a crushing liability disproportionate to the contractor's breach and the actual harm from a security breach involving personal data.

Here is a short list of key issues:

1. Avoid an overly broad definition of "Personal Data". There is no statutory definition of personal data, so some contractors use the broadest definition. One large contractor commonly uses the

Contact

John A. Knab

Related Services

Government Contracts

definition of "any information that may identify a person." Under this broad definition, certain obligations, such as encrypted data transfer requirements, can create unreasonable, even impossible obligations. Do you encrypt every e-mail you send? If not, then an e-mail containing "any information that may identify a person" involved in your IT project can constitute a violation of your encryption obligations for personal data.

2. Avoid unworkable access, storage, transfer, control, and destruction obligations. Some personal data protection clauses impose strict rules for how personal data must be accessed, stored, transferred, controlled, and destroyed. Often, the rules are written for large entities, with a dedicated IT staff and multiple departments or divisions. Either these rules must be tailored to your company or your company must adopt these rules – or a workable compromise must be found. The form language of one large contractor requires subs that have any access whatsoever, even tangentially, to a person's personal data to allow that person the right to access, review, or modify such personal data. Imagine Joe Smith working for HHS in Chicago, IL. For a sub working on a small part of a large project, where such access is possible but not within the scope the sub's work, the obligation to give Chicago Joe Smith the right to access and modify his personal data seems to be an impossible obligation.

3. Remedies must be reasonable and proportionate. Often, personal data clauses require a sub to take certain remedial measures for a data breach – including notifying all data subjects and setting up a 24/7 hotline for data subjects to call. However, few data breaches require such a "full court press." The practice is naturally developing for the parties to assess the severity of breach and take commercially reasonable measures commensurate with the severity. Your clause should reflect this commercially reasonable practice.

4. What are your insurance requirements? Do you have a $10 million policy covering personal data breaches? One large contractor requires that amount, even if the sub has only person on a project. Unless you push back, you will be obligated to acquire that amount. You don't know if you have insurance that covers data breaches? That's a bad idea, too. For your company's own protection, you need an insurance policy that you know will cover data breaches.

5. Be wary of uncapped liability. Many contractors require liability from personal data security breaches to be exceptions to the common clauses that cap liability, such as the "no liability for consequential, incidental, and punitive damages" clause. In other words, if the sub is in any way responsible for a data breach, then there is no limit on the sub's possible liability. Some large companies will agree to a cap equal to the sub's insurance coverage (see $10 million above). Contractors must take this exposure into account in the contractor's cost-benefit analysis of whether to agree to this clause. Moreover, check with your insurance company about such a clause will impact your insurance coverage; some insurance underwriters shy away from extending policies where liability is uncapped.

As stated above, protecting personal data is a worthy goal. However, a contractor need not expose itself to impossible contractual obligations and onerous remedies to do so. By focusing on these clauses, in particular the key issues above, you can negotiate with other contractors to meet that goal in a commercially reasonable manner.

Contact Us

Please contact John Knab at (202) 298-2536, Ben Lambiotte at 202-298-2525, and Julia Holden-Davis at 907-258-2400 for legal advice tailored to your individual circumstances.