MARASHLIAN & DONAHUE, LLC
THE COMMLAW GROUP

INFORMATION PRIVACY AND DATA SECURITY RISK MANAGEMENT CHECKLIST

Intelligent Allocation of Risks and Responsibilities for Data Security Among Business Partners in the Software as a Service, Hosting and Cloud Computing Industries

Strong commitments to data security are essential for third-party vendors who offer services to companies that collect personal information from individuals. Corporations looking to outsource information management in this time of increased interconnectedness and technical complexity will seek vendors who can mitigate security risks. These corporations will expect vendors to take strong actions to protect their customers' data. At the same time, the scope of information collected and the public assurances made with respect to protection of that data are often in the hands of the data collector, not the underlying vendor. Accordingly, vendors and their customers must work together to allocate risks intelligently and create incentives on both sides to protect collected data.

Our firm can assist you as you assess the risks and privacy impact of entering into partnerships that involve the use and collection of protected personal information. Our attorneys can provide guidance each step of the way, from due diligence review of a company's existing practices and procedures to contract negotiation and throughout the life of a contract and the necessary audits and oversight that will continue throughout the partnership.

- **Before you enter into a partnership –**
    - **Build security into the product from the development stage**. Address security issues during the product development process. Early on, identify and address threats and vulnerabilities, design software and hardware controls to address these vulnerabilities, make time for testing to make sure the controls work. Document these efforts. Clearly delineate responsibility for security features of products involved in the partnership.
    - **Software as a Service, hosting and cloud computing companies should include these elements in any risk management process:**
        - **Adopt network controls.** Controls such as firewalls, encryption, user verification, password management, access controls, and maintenance procedures for applications and operating systems should be tested periodically. Develop procedures for recording reports of any identified anomalies.
        - **Separate each customer's data from those of other customers through virtual or physical means.**

MARASHLIAN & DONAHUE, LLC

TELEPHONE: (703) 714-1300
FACSIMILE: (703) 714-1330
EMAIL: MAIL@COMMLAWGROUP.COM
WEB: WWW.COMMLAWGROUP.COM

THE COMMLAW GROUP
1420 SPRING HILL ROAD
SUITE 401
MCLEAN, VIRGINIA 22102

- **Implement stringent hiring procedures and employee training for employees with access to sensitive data.** Procedures such as background checks and drug tests should be routine practices for employees with access to sensitive data. Train employees in the use of passwords, storage practices, and the appropriate use of mobile devices.

- **Deploy physical security systems.** Security systems should include alarms, guards, fire protection devices, and power/communication feeds with backup. Adopt practices to take regular inventories of physical data storage devices.

- **Implement a data retention strategy**.

- **Consider purchasing Data Breach Liability Insurance.**

- **Conduct Due Diligence Review of any Potential Business Partner.**

  - Understand the risk associated with this business partner. Implement partner risk reviews and plan to undertake ongoing reviews over the course of the arrangement. Assess whether you have the resources to undertake this assessment.
  - Find out whether your business partner has policies and practices in place to address privacy and data security. Review personnel practices, physical security, technical security safeguards, and subcontracting plans and practices. Ask how these policies are administered and communicated to employees and subcontractors?

  - If you are an underlying vendor, understand the type of personal information that your potential business partner will collect.

  - Understand the statutory obligations of your potential business partner. Know what privacy framework applies, and whether you will be directly liable under a statute as a business partner of this company.

  - Understand the tension between the value of the services provided and the trade-off for risk assumed in the arrangement by each business partner.

- **Elements of the Contract –**

  - **Understand the statutory obligations** applicable to each contracting party and whether contract provisions are required by law. Generally, an entity cannot contract away its obligation to comply with certain industry-specific regimes, such as GLBA, FERPA, HIPPA, HITECH, and Sarbanes-Oxley.

  - **Oversight**. Build in mechanisms for frequent communication, opportunities

to monitor, audit and oversee operations of business partners.

- **Data Security.** Require your business partner to implement policies and procedures to protect data collected, including:

    - personnel security
    - data collection, use and retention
    - disaster recovery and business continuity
    - compliance monitoring and reporting
    - incident reporting
    - a right to audit
    - termination procedures and requirements
    - review disclaimers and indemnification provisions
    - Address due diligence and contracts with subcontractors

- **What happens if a breach occurs?**

    - **Timing of notification**. Know your notification obligations upfront and requisite timing of notification under law and to protect the companies' reputation.
    - Consider lining up a forensic consultant.

    - Address the costs and clearly delineate responsibilities for:

        - notifying customers and processing claims for damages, including an escalation policy for a clear chain of command after discovery of potential breach
        - public relations
        - credit monitoring services for affected individuals
        - lost business costs
        - cost of regulatory fines and regulatory investigation defense

- **Ongoing monitoring and recordkeeping.** Remain vigilant throughout the life of the contract.

    - Keep good records of sensitive data collected, how it is stored and used.

    - Conduct risk assessments internally and of vendors regularly.

    - Review privacy policies and notices provided to customers who share personal information in reliance on those privacy policies; keep policies updated with material and other changes.

CONTACT US

For more information regarding Marashlian & Donahue, LLC, The *Comm*Law Group's Privacy & Data Security practice, please contact Jonathan S. Marashlian, Managing Partner, or Linda McReynolds, Practice Group Chair:

Jonathan S. Marashlian
Email: jsm@commlawgroup.com
Tel: 703-714-1313

Linda McReynolds
Email: lgm@commlawgroup.com
Tel: 703-714-1318

ABOUT US

Marashlian & Donahue, LLC, The *Comm*Law Group is a full service Washington, D.C.-area law firm serving the comprehensive legal needs of the communications industry. We are experienced in all aspects of federal and state telecommunications law and regulation and represent businesses engaged in the dynamic communications and information technologies industry with virtually all of their legal needs. No matter the scope of our representation, we are committed to offering our clients personal attention and efficient, professional representation. While always keeping your objectives in mind, we maintain our clients' trust and confidence through open and direct communication and valuable, responsive and cost-effective performance.

The *Comm*Law Group is unique among its peers, offering clients a scope of capabilities rarely found in boutique law firms. With a headcount rivaling the Telecom Practice Groups of most major law firms, we boast a team of attorneys, paraprofessionals and consultants possessing the skills, focus and resources necessary to serve the communications law needs of Fortune 100 companies, all without sacrificing the range of services and affordability which makes us the "go to" firm for new entrants and service providers of all sizes.

Information about The *Comm*Law Group and its affiliated consulting firm, The *Comm*pliance Group, is available on their respective websites:

www.CommLawGroup.com

www.CommplianceGroup.com

LEGAL NOTICE