



Data Security & Privacy Compliance Services for Professional Services Firms

A Fixed-Fee Program

Today's landscape for data security and privacy is characterized by increasing complexity. We have more computers, mobile applications, 24/7 connectivity, cross-border data flows and evolving security threats than ever before, while being subject to more stringent legal requirements and security standards. These changes, coupled with the recent surge in high-profile data security breaches and increased global enforcement, mean that data security and privacy compliance can no longer be placed on the back burner—they have become among the highest-priority issues for professional services firms.

Professional services firms are extremely desirable targets for data breaches because they house valuable and confidential data, they have money, and they are not prepared.

Benesch's global data security and privacy compliance team regularly assists professional services firms in their data security and privacy compliance efforts, breach response and mitigation actions, and related issues.

The members of our team are CIPP-certified privacy professionals. We do an extensive amount of data security compliance work helping our clients to comply with a variety of federal, state, local and foreign laws, rules and regulations in jurisdictions including the U.S., Canada and the EU/EEA. These laws, rules and regulations include the EU GDPR and ePrivacy Directive, the EU/US privacy shield, HIPAA/HITECH, Gramm Leach Bliley, COPPA, FTC Act and US FTC Red Flag rule compliance, and Canadian PIPEDA. We also assist our clients with respect to the vast array of data security and privacy technical standards and guidelines with which they must comply, including PCI-DSS, ISO 27001, ITIL, COBIT and NIST standards, as well as with data classification, breach response and mitigation, and the creation and implementation of applicable policies/procedures.

(continued)

Data Security & Privacy Compliance Services for Professional Services Firms

For a fixed fee (dependent upon the size of the firm) we provide the following services:

1. Risk Assessment - We will meet with you to gather the information necessary to perform a review of the existing data security and privacy compliance and document/data retention and destruction programs in place at your professional services firm.

2. Data Security and Privacy Practices - The manner in which professional services firms collect, store, transmit, process, retain and protect data is governed by both state and federal privacy and data security laws, rules and regulations in the United States, as well as the laws, rules and regulations of foreign jurisdictions in which they have operations and employees, and to which they transmit data. We believe it is important that professional services firms fully understand and consider the risks associated with the collection, storage, processing and transmission of personal financial information under current law, and develop and fully implement a comprehensive data security and privacy compliance program across the enterprise.

3. Preparation of Required Policies - Once a final determination has been made about which state, federal and foreign laws, rules, regulations and technical standards apply to your firm, we will prepare a comprehensive policy manual containing those data security and privacy policies and procedures that are required under applicable law.

4. Review of Contracts - It is vitally important that professional services firms' relationships with third-party vendors comply with all applicable federal and state laws, rules and regulations and with the firms' new security and privacy and record retention/destruction programs. We will complete a full legal review of all third-party contracts that relate to the collection, storage, processing and transmission of personal information and data to determine whether these contracts are in compliance with applicable law and the company's policies and procedures, and to assist our professional services firm clients in identifying areas of noncompliance or deficiencies that should be revised or amended if possible.

5. Employee Education and Training - Critical to comprehensive data security and privacy compliance is effective employee education and training regarding the policies and procedures established by your professional services firm. Once these policies and procedures have been finalized and adopted, we propose to conduct on-site and/or remote (i.e., via video conferences or webinars) education and training programs for all applicable employees regarding compliance with the new policies and procedures that your firm has implemented. We intend to take a modular approach to education and training, treating each aspect of the data security and privacy compliance program as a separate module. We will provide your professional services firm with a menu of available education and training modules to choose from.



For more information, please contact MICHAEL D. STOVSKY
mstovsky@beneschlaw.com | 216.363.4626