

Data Security, Privacy and Information Governance: Initial Risk Assessment

The Initial Legal Risk Assessment is a Cohen & Grigsby service to assist our clients with a preliminary analysis of their business practices and risk profile as they relate to the creation, use, protection, retention and destruction of sensitive information. Using information we gather as part of the initial risk assessment, we are able to help business leaders better understand their risk and risk management as it pertains to sensitive information generated by, entrusted to, held by and otherwise controlled by the organization. We present our findings in a report and presentation that contains (i) an overview of various information-related legal obligations as they apply to the company; and (ii) an assessment of the company's current practices and controls designed to comply with those various obligations.

After completing the Initial Legal Risk Assessment, our clients are better able to prioritize their objectives and marshal their resources in a manner that reflects the evolving demands of proper information governance in the current business environment and legal landscape. With our streamlined, multi-disciplinary approach to data privacy, security and information law, we can be there with you every step of the way.

We tailor our Initial Legal Risk Assessment to the size and needs of our clients. As a general matter, however, we typically perform the following preliminary analyses:

Sensitive Data Identification

We work with our client to think broadly and identify the types and nature of sensitive data (e.g., PII, PCI, ePHI, company trade secret and proprietary data, employee/HR information, payroll information, controlled defense information, consumer credit information) within the company's possession, custody or control that may be subject to legal obligations relating to protection, retention or destruction of that data.

IT Environment Assessment

We help our client assess the appropriate scope of review for the company's IT environment to identify the various repositories, volume and accessibility of documents and electronically stored information within the company's possession, custody or control (including information that is self-hosted, cloud-hosted and third-party entrusted).

Geographic Footprint Assessment

We review the company's geographic footprint to identify jurisdiction-specific obligations (e.g., state specific legal obligations (e.g., California, Massachusetts, New York), EU Data Privacy, Canada / CASL) relating to the protection, retention or destruction of sensitive information within the company's custody, possession or control.

Third-Party Contract Review

We identify the company's contracts with third-party vendors and service providers that have access to or are entrusted with the company's data (e.g., service agreements, non-disclosure agreements).

We identify contracts with third-party customers and business partners that have entrusted the company with third parties' data (e.g., service agreements, non-disclosure agreements, subcontracts).

Internal Contract and Policy Review

We identify employee contracts as well as internal policies and controls governing the intake, maintenance, retention, protection and destruction of information by the company's employees (e.g., non-disclosure agreements, assignment of inventions, employee handbooks, social media policies, technology use policies, cybersecurity policies, data backup and business continuity plans).

Advertisement Assessment

We identify business-related communications and marketing referencing the company's use and protection of third parties' information.

Litigation Readiness Assessment

We identify the company's policies and procedures governing the implementation, maintenance and cancellation of litigation hold notices. Further, we identify policies and procedures governing the company's identification, collection, search, analysis and production of documents and electronically stored information in connection with litigation and other adversary proceedings.

Insurance Policy Review

We identify and assess insurance policies providing cybersecurity and information management related coverage.

Bruce C. Chiu



Co-Chair,
Data Security, Privacy and Information
Governance group
412-297-4622
bchiu@cohenlaw.com

Fridrikh V. Shrayber



Co-Chair,
Data Security, Privacy and Information
Governance group
412-297-4612
fshrayber@cohenlaw.com

ABOUT COHEN & GRIGSBY

Since 1981, Cohen & Grigsby, P.C. and its attorneys have provided sound legal advice and solutions to clients that seek to maximize their potential in a constantly changing global marketplace. Comprised of more than 140 lawyers, Cohen & Grigsby maintains offices in Pittsburgh, PA and Naples, Fla. The firm's practice areas include Business Services, Labor & Employment, Immigration/International Business, Intellectual Property, Real Estate & Public Finance, Litigation, Employee Benefits & Executive Compensation, Estates & Trusts, Bankruptcy & Creditors Rights, and Public Affairs. Cohen & Grigsby represents private and publicly held businesses, nonprofits, multinational corporations, individuals and emerging businesses across a full spectrum of industries. Our lawyers maintain an unwavering commitment to customer service that ensures a productive partnership. For more information, visit www.cohenlaw.com.

The hiring of a lawyer is an important decision that should not be based solely upon advertisements. Before you decide, ask us to send you free written information about Cohen & Grigsby's qualifications and experience.