SEYFARTH SHAW

Global Privacy & Security Team

Privacy Compliance

In today's climate of increasing federal audits and regulatory oversight, our clients rely on Seyfarth's Global Privacy & Security (GPS) Team to ensure compliance with major privacy laws and avoid costly penalties.

In the age of the security breach, it is no longer enough to be reactive to threats to privacy and security. By understanding the need to be proactive in demonstrating compliance, we assist our clients in analyzing their practices with respect to data collection and use, transfer and retention, including maintaining information in the cloud. By mitigating the risks associated with managing the capital asset which is data, we support our clients in implementing state-of-the-art, cutting-edge compliance programs to preserve and protect personal information, as well as training clients on proper practices. Looking at an organization's practices holistically enables us to help our clients establish internal controls designed to maintain the security of a business' vital information. Such steps help our clients to avoid privacy glitches and security breaches and the costly litigation, fines, audits and loss of goodwill and/or trust that they can cause.

International Privacy Compliance. Members of our team have experience in developing policies and procedures for clients doing business in Europe, Asia, the Middle East, Africa, Latin America and Canada, as well as, of course, the United States.

We have considerable experience in creating and implementing strategic international privacy compliance programs for multinational organizations with respect to the collection, use, and transfer of personally identifiable information of consumers, vendors, employees and other

Our Capabilities:

Global Privacy and Security Capabilities | **Privacy Compliance Capabilities** | **Privacy Litigation Capabilities** | **Incident Management Capabilities** | **Vendor & Technology Transaction Capabilities**

- ☑ Major privacy law compliance (HIPAA, COPPA, FCRA, FACTA, TCPA, CAN-SPAM, etc.)
- ☑ Global HR-related data management
- ☑ Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules system
- ☑ Co-regulatory/self-regulatory programs
- ☑ Employee privacy and employer compliance
- ☑ HIPAA training of workforce
- ☑ Background screening
- ☑ Encryption requirements (state and federal)
- ☑ "Privacy Officer" development and best practices
- ☑ International data transfers
- ☑ EU data protection directive (and local implementing laws)
- ☑ Bring your own device (BYOD) and social media policies
- ☑ Disposal of personal information

individuals. These include compliance with laws in the European Union, Asia, Latin America, and other countries with stringent data protection requirements.

In undertaking these projects, we have prepared global, regional and country-specific privacy policies, monitoring and electronic use policies, whistleblower policies, intra-company contracts, and contracts for service providers to process personally identifiable information on behalf of our clients. We have coordinated filings, notifications, and registrations related to privacy compliance with local data protection authorities, and self-certification with the United States Department of Commerce for Safe Harbor.

We closely monitor recent developments in global privacy laws, for example, individual consent to processing, eDiscovery, whistleblowing, collection of diversity data/sensitive personal information, and background screenings.

EU Data Protection Directive. On a daily basis, we assist clients to manage their data protection obligations stemming from the European Union's 1995 Directive regulating the privacy and protection of personally identifiable data throughout Europe ("European Data Protection Directive"). We are familiar with the myriad of issues that arise as a consequence of each European Economic Area member state adopting its own legislation interpreting the European Data Protection Directive, and the different approaches that the data protection authorities have to registrations, notifications, audits, enforcement, and penalties. We have worked with local counsel throughout Europe to determine compliance requirements for our clients. We also advise our clients on how to transfer personal data out of the EU to countries that have not been deemed to have "adequate protections" as required by the European Data Protection Directive.

Employee Privacy and Employer Compliance: BYOD and Social Media Policies. We monitor compliance with quickly changing and evolving social media privacy laws and regulations, and we develop compliant policies and best practices regarding social media use, including employee-use privacy policies that follow National Labor Relations Board (NLRB) guidelines. We also help clients manage where and how electronic information is stored and establish information governance programs that ensure compliance with litigation discovery, data security, and privacy obligations, as well as manage risks associated with the implementation of new technologies.

FCRA. Attorneys on our team have a special emphasis on the Fair Credit Reporting Act (FCRA) and state laws affecting background screening. We counsel both employers and providers (resellers and consumer reporting agencies) of background information on compliance requirements under the FCRA and related state laws, and have been involved in litigation regarding these issues.

Internal Investigations. Management of employees often entails investigating and reviewing conduct. Our attorneys have significant experience in both developing monitoring and review programs, and helping our clients manage any internal investigations which may be necessary.

HIPAA Privacy and Security. Whether large or small, healthcare plans count on Seyfarth to provide a range of services that includes implementing and enforcing how the group health plan, the employer and plan providers can use and disclose protected health information, as well as communicate with plan participants, the U.S. Department of Health and Human Services (HHS) and sometimes the media, in the event that protected information has been erroneously disclosed. Additionally, we bring a wealth of experience in amending healthcare plans, compliance policies and procedures, and provider agreements. Apart from reviewing and revising policies, we ensure that employees are accurately trained and that health care participants are properly notified of their individual rights.

Our attorneys work with clients to identify compliance issues before they become a problem, help them establish systems for thorough record-keeping, minimize disruptions to human resources and benefits, and provide practical advice and guidance backed by comprehensive administrative policies. Along the way, we help our clients adjust their policies in accordance with changes in the laws. Throughout, our attorneys bring the same unique level of innovation and problem solving for which Seyfarth is known.

Seyfarth's cutting-edge approach has allowed us to develop a number of tools that clients can use to achieve compliance, including our flat-fee HIPAA subscription service that provides automatic updates for new regulatory developments. Additionally, we provide personalized on-site consultation, training and interviews to determine the location and uses of protected health information. We also help our clients formulate comprehensive policies that provide guidance on day-to-day operations and the processing of requests and complaints. Finally, we provide a customized set of frequently used regulatory forms and business associate agreement templates.

Likewise, our benefit plan clients gain from Seyfarth's astute guidance in computer and technology contracts, e-health initiatives, intellectual property, medical records retention and compliance for insurers, providers, vendors and other third parties, and with state-to-state privacy laws.

Gramm-Leach-Bliley Act Privacy and Security. Banks and other financial services companies have specific obligations under the Gramm-Leach-Bliley Act (GLBA) to protect the non-public personal information of their consumers from disclosure to unauthorized parties. Additionally, any company that accesses or stores such information will also have privacy and security obligations. Our attorneys have experience with building and implementing GLBA privacy and security programs. We work with our clients to develop and implement policies, standards, and procedures necessary to comply with the panoply of legal requirements. We also defend banks and other companies accused by government authorities or private litigants of violating such legal requirements.

Consumer Privacy Law. Most companies are expected to post privacy policies on their websites and mobile applications. California actually *requires* the posting of a privacy policy for websites and mobile applications. Under both state and federal law, companies must comply with the promises set out in these publicly facing policies. We help companies draft these policies, as well as put in place processes and controls to comply with these policies. Additionally, when a company wants to develop a new line of business, or a new way to monetize personal data it has collected via its websites or mobile applications, our attorneys provide valuable advice on what kind of privacy and security risks may be present, and how to mitigate such risks.

Along with privacy law, many states have started including affirmative security requirements on companies who process personal information. Massachusetts incorporated the Payment Card Industry's Digital Security Standard ("PCI-DSS") into its regulatory implementation of its security breach statute. We advise our clients, across a number of industry sectors on what is required for compliance with these security requirements. Our attorneys understand not just the process controls, but also the technical controls (like encryption) necessary for a compliant privacy and security program.

Track Record of Results

- Represented a U.S. multinational leader in the technology infrastructure industry in a global privacy project that centered on the flow of the company's workforce and contractor data across 130 countries. We worked with the company to develop compliance tools including global policies, agreements, notices, consents, procedures, processes, guidelines, codes, forms and standards, to define the company's global approach to protect the personal data of nearly 100,000 workers. We developed a practical and innovative strategy to be legally compliant and to meet the company's commercial needs. The project involved complex issues requiring an understanding of the legal requirements across multiple jurisdictions, the commercial constraints within which the company operates, and the company's values and goals.

- Represented a U.S. multinational engineering and construction company in a global privacy compliance project that involved assessing the company's flows of personal data across its global operations—across 50+ countries in Europe, Asia, North, Central and South America, the Middle East and Africa—and designing and implementing a compliance program to ensure the lawful cross-border transfer of the data. We advised on the issues and designed the compliance program and are currently assisting with its implementation, including preparing policies, notices, consents, agreements and training materials.

- Represented a U.S. multinational corporation in the memory technology industry within a global data privacy project that involved auditing the company's collection, use, transfer, disclosure, and retention of HR data among its operations throughout Asia, Europe, North America, Central America, South America, and the Middle East, and formulating a strategy to ensure the company's lawful cross-border transfer of that data. We worked with the company on its certification with the U.S. Department of Commerce's Safe Harbor Program, and prepared cross-border and third party contracts, employee notices, and global policies, procedures and guidelines reflecting the company's standard for protecting personal data. We also addressed the company's global registrations with Data Protection Authorities.

- Represented a U.S. multinational public relations firm with a global privacy compliance project that involved assessing the company's flows of personal data across its global operations—including human resources data, client data and consumer data—from a wide variety of sources. Our team helped to conduct the assessment, advised on global policies and procedures as well as improvements to the client's existing measures and documentation.

Our attorneys work with clients to identify compliance issues before they become a problem. Along the way, we help our clients adjust their policies in accordance with changes in the law.

- Represented a U.S. biopharmaceutical company with its global privacy and data protection program development and preparation for Safe Harbor filing. Our team has worked to update and finalize complex policy and operational infrastructure for compliance with US-EU Safe Harbor Framework, while ensuring scalability of those elements into a global solution. This included electronic document and eDiscovery elements as well as regulatory requirements.

- Represented TRUSTe/U.S. Department of Commerce in the finalization of the APEC Cross Border Privacy Rules Framework. Served as initial drafter and primary editor for the U.S. delegation to APEC to develop an interoperable framework for privacy protections across 21 different economies in the Asia-Pacific region. Also instrumental in ensuring other Economy Delegation's Trustmarks were driving the same rule set. Motivated involvement of EU Privacy regulators in APEC process to eventually achieve interoperability between APEC and EU privacy enforcement systems

- Counseling a *Fortune* 500 fast food restaurant company on privacy and data security issues relating to the company's development and implementation of international employment and social networking websites. This includes their international HRIS and compensation system, as well as an internal corporate Facebook-like site. In addition, we have revamped the client's background screening policies, procedures and processes. Our client is one of the world's largest fast food restaurant companies with 36,000 restaurants in more than 110 countries.

- Represented a medical information management company in designing and implementing its HIPAA privacy and security compliance program for its health plan. Because this client was also required to comply with the HIPAA privacy and security requirements at its corporate level (due to the nature of its business), we designed and implemented a compliance program that harmonized with its corporate compliance efforts. Finally, we designed and delivered the required training by webcast, allowing the client's employees in multiple states to attend simultaneously. These efforts resulted in minimal duplicative compliance requirements and significant cost savings to the client.

- Represented a for-profit education company in a nationwide pattern or practice lawsuit filed by the Equal Employment Opportunity Commission (EEOC) claiming that our client's practice of checking credit histories of job applicants and employees was racially discriminatory and discriminated against a class of African-American applicants and employees. This was the first (and largest) case of its kind to be brought by the EEOC and millions of dollars were at issue. Of significance, when the EEOC brought this case back in 2010, the agency made it well-known that it was a test case challenging background check practices during the hiring process as discriminatory on the basis of race. Had the EEOC prevailed, the EEOC would have used a similar tactic to bring pattern or practice litigation against employers nationwide. Shutting down this case through a complete summary judgment victory has saved employers nationwide from systemic litigation over hiring screens.

SEYFARTH SHAW

www.seyfarth.com