

Cyber and Data Security

Overview

AP&S' Cyber and Data Security practice group recognizes the importance of technology to our client's businesses. For that reason, we provide our clients with the advice and tools they need to protect themselves in the use of state-of-the art technology. We also recognize that no business – large or small – is immune to a data breach or computer theft. When data breaches occur, we work hand-in-hand with our clients and cybersecurity professionals to investigate and respond appropriately.

Our multidisciplinary team includes attorneys in our Business & Corporate Group who review and negotiate technology, software and cybersecurity service agreements, attorneys in our Labor & Employment Group who develop workplace policies designed to protect against computer theft and data breaches, attorneys in our Health Care Group who advise clients on compliance with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and corresponding state law, and attorneys in our Litigation Group who routinely litigate computer crimes and privacy and data protection matters in federal and state court.

Areas of Concentration

- Data breach risk mitigation
- Data breach response and notification
- Health information privacy
- Employee data privacy
- Consumer data privacy
- Cybersecurity concerns for financial institutions
- Financial data privacy
- Litigating computer crimes and privacy and data protection matters in federal and state court

Experience

- Guided an international company through an investigation and response to a cybersecurity breach.
- Developed workplace policies with a wide range of controls to protect against computer theft and data breaches, including data usage policies, computer and network usage policies, data retention policies, social media policies and bring your own device policies.

© 2026 Adler Pollock & Sheehan P.C. All Rights Reserved.

- Defended a global retailer against threatened class action alleging improper collection and misuse of personal identifying information in violation of data privacy laws.
- Defended against claims of interception of electronic communications under federal and state law related to data allegedly received as a result of the installation of key logger software.
- Defended against and prosecuted civil claims for computer crimes under various states' laws.
- Assisted international clients with satisfying their obligations under the General Data Protection Regulation ("GDPR") while also meeting their discovery obligations in United States courts.
- Assist companies with the development of privacy policies.
- Reviewed and negotiated software, technology and cybersecurity service agreements to ensure proper data safeguards.
- Advised clients regarding the risks inherent in new technologies, artificial intelligence and the Internet of Things.
- Defended banks and financial securities companies in litigation brought by customers who incurred losses as a result of cybersecurity breaches.
- Represented health care providers in compliance with HIPAA, and state law when responding to subpoenas and document requests.
- Advised healthcare providers in connection with HIPAA, Business Associate Agreements, and state law data breach notifications.
- Advised clients regarding their need for cybersecurity insurance and represent insurance brokers who are versed in cybersecurity insurance issues. Provide coverage opinions to insurance carriers that provide cybersecurity insurance.

Seminars/Publications

Publications

- Ethical Considerations in the Global Data Environment, Safeguarding Client Information in 2018 CLE, May 2018.
- Legal Considerations for the "Smart" Workplace, AP&S CLE, April 2017.

© 2026 Adler Pollock & Sheehan P.C. All Rights Reserved.