

Data Privacy, Data Protection, and Cybersecurity

In a privacy environment that often lacks extensive precedent, our attorneys assist with developing best practices based on commonsense risk analyses. Our attorneys draw on substantial experience, in-depth certifications, and technical acumen to guide clients in structuring solutions that reflect the latest privacy and security mandates. Though data protection and cybersecurity issues carry considerable risk – legal, financial, and reputational – with proper attention and the help of our attorneys, these areas may be turned into a valuable competitive advantage.

Risk Minimization Through Proactive Compliance

Clients look to us to advise them on their current and planned privacy practices – how they interact with consumers, how they collect and use data, how they build new services, when and how they make disclosures – while keeping a sharp focus on their regulatory obligations. As our clients decide on their own internal and external policies, enter into new agreements with vendors and customers, and leverage data issues in M&A transactions, we advise them on the likely effects of these arrangements and how to minimize risk. In an area of law that is not fully evolved, we counsel clients on best practices and any self-regulatory requirements imposed by their industry. Equally important, our attorneys assist with the operational challenges that arise from new compliance requirements, and work in tandem with clients throughout the implementation process.

Multi-Jurisdiction Advice

Our attorneys help synchronize varying requirements under EU and U.S. data protection and privacy laws, structuring business strategies that reflect the latest privacy mandates and commonsense risk analysis. We regularly advise clients on multi-jurisdictional data protection issues, including GDPR, CPA, CCPA, and an ever-expanding list of state and industry-specific privacy laws.

Ongoing Compliance and Development Monitoring

The potential for misuse of personal information has triggered legislative and regulatory action worldwide, and the risks are high. Privacy laws are continually evolving, vary by jurisdiction, are interpreted unpredictably, and are in a constant state of flux. Even the most well-meaning company can make a false step as it captures, uses, transfers, and discloses personal information. For this reason, our attorneys regularly review our clients' current practices and reconcile them with the latest developments.

Specific Data Privacy, Data Protection, and Cybersecurity Services

Our attorneys regularly handle an organization's overarching compliance and discrete data-related needs. Some of the discrete tasks our attorneys handle include:

- Cross-border data transfer (both intra-group and with third parties)
- Binding Corporate Rules (BCR) and APEC Cross-Border Privacy Rules System
- Privacy and cybersecurity policies
- Privacy and cybersecurity audits
- Data security breach preparedness and response
- Privacy-related claims and disputes
- Privacy statements for online activities
- Employee privacy

- Financial privacy
- Healthcare privacy
- Marketing policies
- Privacy and cybersecurity aspects of cloud computing and other sourcing arrangements
- Data processing and data transfer agreements
- Privacy aspects of investigations and e-discovery
- Due diligence and warranty negotiation for M&A
- Special data categories, including those designated by the Health Insurance Portability and Accountability Act (HIPAA), Children’s Online Privacy Protection act (COPPA), Gramm-Leach-Bliley Act (GLBA), and others

Our privacy team includes attorneys with industry-leading certifications, including Certified Information Privacy Professional/United States (CIPP/US) and Certified Information Privacy Manager (CIPM) distinctions. These certifications are a standard in obtaining the skills and expertise required throughout the life cycle of its operational life cycle.

