

PRACTICE

Data Privacy & Cybersecurity

Benesch's Data Privacy & Cybersecurity Practice Group helps organizations navigate the rapidly evolving privacy, cybersecurity and AI regulatory landscape with clarity and confidence. Drawing on deep in-house experience and experience across regulated and data-rich industries, we provide practical strategies that operationalize compliance, manage enterprise risk and support responsible innovation.

Recognized

by Best Law Firms®



24/7

Data Breach Hotline:

800.865.2494

What We Do

U.S. STATE PRIVACY COMPLIANCE

Comprehensive U.S. state privacy law compliance (including CCPA), sensitive data requirements, consumer rights operations, data subject access requests and data minimization strategies

AI GOVERNANCE AND RESPONSIBLE INNOVATION

AI risk assessments, governance frameworks, model oversight, use of data in training and evaluation, and compliance with emerging state and global AI legislation and industry standards

PRODUCT PRIVACY AND AI DEVELOPMENT

Privacy and security review of new products, features and AI models, including data flow analysis, privacy-by-design implementation, model development risk assessments and product-level data governance

MARKETING TECHNOLOGY AND TRACKING COMPLIANCE

Tracking technologies across digital and physical environments (cookies, pixels, in-store location tracking, cross-device identifiers), CIPA exposure, targeted advertising compliance, retail media networks and consent mechanism design

PRIVACY AND DATA PROTECTION CONTRACTING

Data processing agreements, AI addenda, privacy/security schedules, data-sharing arrangements, joint data collaborations and commercial privacy terms

INTERNATIONAL DATA TRANSFERS AND GLOBAL COMPLIANCE

Cross-border data transfers (e.g., SCCs, BCRs, TIAs), adequacy determinations and global privacy program alignment across GDPR, PIPEDA and APAC frameworks

DATA SECURITY AND READINESS

Security program development, readiness assessments, tabletop exercises, vendor security practices and ongoing risk mitigation

INCIDENT RESPONSE

Breach response, notification analysis, regulatory inquiries and multi-jurisdictional coordination

HIGH-RISK DATA GOVERNANCE

Biometric, geolocation, children's data, health and financial data, and other high-risk data categories

STATE REGULATOR ENGAGEMENT

Proactive and reactive engagement and compliance counseling with state attorneys general and privacy regulators, response to regulatory inquiries, compliance strategy coordination, and state-specific enforcement risk mitigation

Who We Serve

- Consumer Products, Retail and E-Commerce
- Technology, SaaS and AI/ML Companies
- Sports, Entertainment and Media
- Health Technology and Digital Health
- Financial Services, Payments and Fintech
- Hospitality and Real Estate
- Sustainability, Energy and Emerging Industries

Thought Leadership

Through datameetsworld.com, our team provides practical insights on global privacy developments, CIPA exposure trends, AI regulatory frameworks and emerging compliance requirements.

Representative Matters

- ▶ Develop comprehensive AI governance programs for financial services, SaaS and technology companies integrating proprietary and third-party AI into customer-facing products, including regulatory compliance frameworks, AI-specific contract addenda, product design counseling, risk disclosure strategies and automated decision-making oversight processes.
- ▶ Respond to security incidents involving generative AI platforms, unauthorized data access and sensitive data exposure across financial services, healthcare and technology sectors, including breach notification analysis, C-suite and board presentation, forensic coordination, litigation strategy and comprehensive remediation planning.
- ▶ Advise retail, consumer, digital media and hospitality companies on tracking technologies across web, mobile and physical environments, including in-store location tracking, retail media networks, loyalty programs, cross-device marketing, CIPA exposure mitigation and consent framework design.
- ▶ Design scalable, portfolio-wide privacy programs for companies integrating multiple acquisitions across consumer, technology and media sectors, including harmonized governance under omnibus state privacy laws and COPPA, vendor management frameworks, and post-acquisition compliance integration supporting continued deal activity.
- ▶ Counsel SaaS, AI/ML and emerging technology companies on privacy and security review of new products and features, including data flow analysis, model development risk assessments, training data governance, profiling and segmentation, and biometric and geolocation implementations.
- ▶ Build stand-alone privacy compliance programs for newly independent companies, spinouts and carve-outs, including global regulatory assessments, risk tolerance frameworks, litigation exposure mitigation (including CIPA response), and separation from legacy parent company data systems and policies.
- ▶ Advise sports, entertainment and media organizations on privacy and AI governance for advanced analytics, fan engagement platforms, athlete and talent data initiatives, data-sharing partnerships, retail and venue integrations, and connected technologies.
- ▶ Support large-scale strategic acquisitions and sales across sports, entertainment, beauty, digital media, hospitality, sustainability, biotech and consumer product sectors by leading privacy and data security diligence, sensitive data assessments, targeted advertising risk reviews, AI/ML capability evaluation and post-closing remediation planning.
- ▶ Advise payments processors, fintech platforms and financial services start-ups on privacy program development from formation, including tailored terms of service and privacy policies addressing payment platform risks, cross-border data flows, consumer protection obligations, and privacy-by-design integration for regulatory readiness and investor diligence.
- ▶ Partner with state attorneys general and privacy regulators on proactive compliance strategy, pre-launch reviews and regulatory risk assessment, as well as respond to formal inquiries and investigations involving tracking technologies, consumer consent, dark patterns and multi-state privacy law coordination.