

Partner, London

Cybersecurity and Data Privacy; Artificial Intelligence



T: 44.20.7519.7101
nicola.kerr-shaw@skadden.com

Education

Post Graduate Diploma In Law,
University of Oxford, 2010

Legal Practice Course,
BBP Law School, 2007

LL.M., University of Cambridge, 2005

Bar Admissions

England & Wales

Nicola Kerr-Shaw advises global clients on cybersecurity, data privacy, AI and emerging technology regulation and online safety, helping organizations manage risk, respond to complex incidents and translate regulatory challenges into actionable business strategies.

Ms. Kerr-Shaw has extensive experience advising global clients on complex, high-stakes matters at the intersection of technology, regulation and operational risk, with a focus on cyber preparedness, crisis management, incident response and compliance with evolving AI, privacy and online safety laws.

Drawing on more than a decade of in-house experience at a leading global financial institution, Ms. Kerr-Shaw brings a practical, business-oriented perspective to building and implementing sophisticated legal governance frameworks for cybersecurity, data and AI. She has led enterprise-wide cyber incident responses, coordinated regulatory engagement across multiple jurisdictions and designed simulation exercises and tabletop programs to prepare organizations for high-pressure, fast-moving crises.

Her practice also spans emerging technology and fintech, counseling clients on cross-border data transfers, consent, monitoring, digital transformation initiatives and AI governance, and helping to translate regulatory complexity into clear, actionable strategies that align with business objectives.

Ms. Kerr-Shaw is recognized by industry outlets for her collaborative approach, clear communication and ability to guide clients through challenging circumstances. She has been repeatedly named one of *Lawdragon's* 500 Leading Global Cyber Lawyers and was honored as one of *Cybersecurity Docket's* Incident Response Elite 2026.

Ms. Kerr-Shaw's experience includes advising on:

- strategic responses and breach coaching with regard to numerous high-stakes and complex cyberattacks, including on critical infrastructure, financial services and high-profile commercial entities
- cybersecurity preparedness and resilience, such as in response to new regulatory obligations, including designing incident response plans, leading tabletop exercises and coordinating with in-house legal teams on rapid, coordinated response strategies
- strategies with regard to online safety product counseling and regulatory investigations
- complex data privacy and compliance matters, including cross-border data transfers, consent management, data subject access requests and alignment with global regulatory regimes
- digital transformation and AI, including with regard to governance, regulatory compliance and contractual frameworks
- mergers and acquisitions, including transactions involving technology-driven, startup and fintech companies, with a focus on cyber risk, privacy and AI
- technology and data-related disputes and investigations, including with regard to cyber fraud, data breaches and insider threats