Nicola Kerr-Shaw

Skadden

Counsel, 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 represents a wide range of global clients in matters pertaining to artificial intelligence (AI), cybersecurity, data and privacy, and complex technologies. She works in tandem with companies to creatively and effectively help them achieve their commercial goals.

Ms. Kerr-Shaw has extensive experience assisting clients with cyber preparedness, crisis management and incident response issues, while ensuring compliance with various obligations under privacy laws, financial regulations and other regulatory requirements. In recognition of her work, she has been named one of Lawdragon's 500 Leading Global Cyber Lawyers.

Prior to joining Skadden, Ms. Kerr-Shaw worked for more than a decade at a major worldwide financial institution, where she built sophisticated global legal governance structures for cybersecurity, privacy, data and AI from the ground up and prepared for and led cyber incident responses for the enterprise-wide legal team. In this capacity, she coordinated the company's legal approach while maintaining communications with various regulators worldwide.

Ms. Kerr-Shaw has extensive experience advising U.K. and EU companies on new and emerging financial technology, utilizing her knowledge of financial regulations and data- and technology-focused laws to effectively counsel clients.

She has advised on complex global outsourcing and offshoring projects, on both an internal and external scale, assisting clients on legal and regulatory requirements, internal governance and contractual frameworks.

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

- complex, high-stakes intellectual property, procurement and outsourcing matters, including issues involving AI, cyberattacks, privacy laws (such as the General Data Protection Regulation), technology and digital contracts, trademarks, brand strategy, software (including open source), distributed ledger technology and digital payments
- responses to global cyberattacks, technology failures and data breaches, including resultant litigation, regulatory notifications, considerations of privilege and communications with staff, regulators and other third parties
- cyber response preparations and training, including hosting tabletop and simulation exercises, drafting incident response plans and organising legal teams to ensure swift and appropriate action
- a wide variety of complex and challenging data issues, including those involving consent management, data transfers, monitoring, cross-border data subject access requests and considerations regarding potential conflicts with other laws and regulations, including sanctions regimes
- digitalisation initiatives and novel technologies, including internal governance, regulatory implications and contractual frameworks
- mergers and acquisitions, including transactions involving startup and fintech companies, particularly in deals in which technology, IP or complex IP licensing arrangements were key considerations
- disputes involving cyber fraud, trademark and copyright infringement, and breaches of licensing, among other issues