# Artificial Intelligence

EPSTEIN
BECKER
GREEN

Data is going digital, devices are going mobile, and technology is revolutionizing nearly every aspect of how we work and care for one another. Digital information and technology are key drivers in today's economy, but data or technology, independent of one another, are insufficient to solve the complex problems we face. Artificial intelligence ("AI") technologies that leverage data show enormous promise to unlock insights about how to improve the way we work and care for one another.

## AI That *Works* for Us

Ever-changing legal requirements coupled with rapid advances in technology have posed challenges and opportunities for employers. Employers face restrictions on the types of employee and job applicant information they can collect and utilize to make informed and defensible business and employment decisions. These restrictions relate to areas such as background checks, employee monitoring, the transfer and maintenance of employee data, and drug testing. The responsible use of AI in these contexts can be transformative to support employer decision-making at scale, but this requires navigating ever-evolving privacy and data protection rules.

## AI That *Cares* for Us

The health care and life sciences industries are other prime examples of where AI may be transformative. These industries continuously endeavor to identify and deliver innovative, cost-effective, personalized, and high-quality therapies and models of care. Fortunately, the industry is highly digitized and has robustly adopted health information technology to develop, provide, and pay for care. AI may help to reduce costs, increase efficiency, and improve quality and safety in ways that positively augment innovation and delivery of care. Yet, implementing AI will require navigating onerous privacy and data protection rules specific to these industries.

## AI That We Can *Trust* Through Privacy and Data Protection

Managing privacy and data protection risks proves critical to establishing trust in AI technologies. The success of AI depends on robust and iterative training through processing of vast quantities of data, which often poses privacy and data protection implications. Yet, privacy and data protection requirements remain complex and ever evolving, and may vary depending on the industry, particular application of AI, and the data processed through AI. This results from the multitude of legal regimes around the globe and numerous regulatory changes on the horizon.

# Why EBG?

Epstein Becker Green ("EBG") is able to leverage its vast experience in privacy and security matters to counsel clients, including countless health care entities, health information technology companies, as well as employers across a wide variety of industries, on issues impacting AI development and adoption.

The firm's Privacy, Cybersecurity, and Data Asset Management Group advises clients that use AI technologies on how to comply with privacy-related federal and state laws, rules, and regulations, as well as how to navigate complex, overlapping, and sometimes conflicting privacy and data protection regimes, including privacy requirements in Canada, the European Union (including the GDPR and its precursors), Australia, and a number of other jurisdictions. Moreover, our group uses its institutional knowledge to provide effective strategies to help clients navigate AI privacy and data protection issues related to transparency and individuals' rights, data governance and minimization, bias and fairness, accountability, and cybersecurity. These strategies are designed to manage risk associated with privacy and security breach, government enforcement, and possible class action litigation.

Our Privacy, Cybersecurity, and Data Asset Management Group includes industry-recognized privacy and security professionals and attorneys who blend privacy proficiency with data protection services to assist clients with integrating AI technologies into their operations. Members of this group maintain various credentials, including:

- Certified Information Systems Security Professional ("CISSP")

- Certified Information Privacy Professional ("CIPP")

- Certified Professional in Health Information Management Systems ("CPHIMS")

- Health Information Trust Alliance ("HITRUST") Common Security Framework Practitioner ("HITRUST CSF Practitioner")

## Representative Experience

- Conducted privacy and security due diligence of an offshore AI developer and technology for integration into revenue cycle management operations

- Negotiated contractual privacy and data protection requirements for workforce management and recruitment AI technology

- Developed data governance program and de-identification strategies for an AI-powered data analytics platform for the life sciences industry

- Provided counsel on privacy and data protection requirements for a cloud-based AI technology used to care for patients with degenerative cognitive conditions

- Provide privacy and data protection guidance on using AI-powered natural language processing tools to curate personal information

Learn more at https://www.ebglaw.com/artificial-intelligence/.