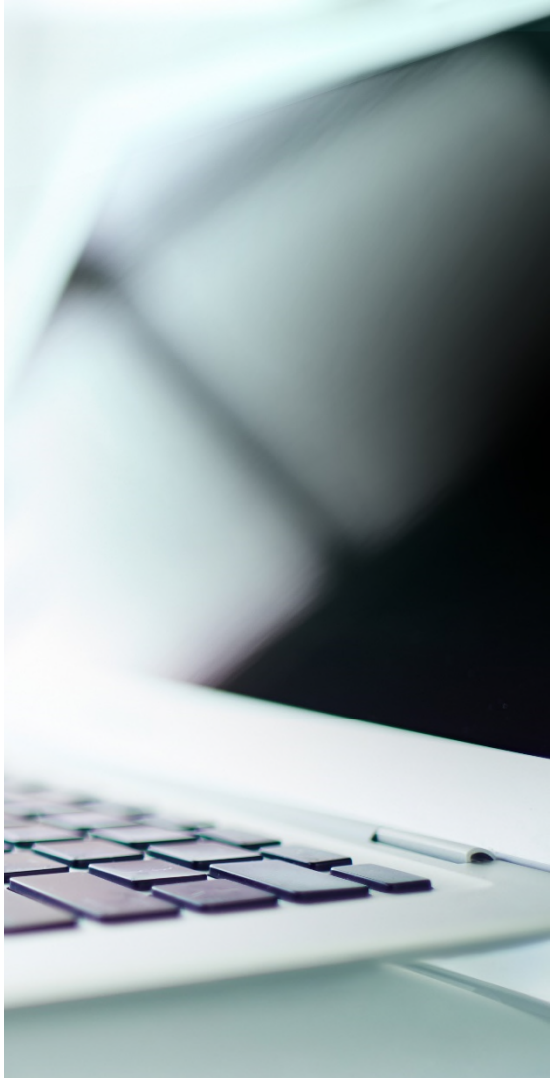
CYBERSECURITY & DATA PRIVACY

TO ENHANCE GLOBAL DATA INNOVATION

Awareness Training

MAYER | BROWN

Table of Contents



Overview

The Global Data Innovation group is specifically focused on providing special counsel services to officers and directors to help them navigate their role with regard to data stewardship and strategy. Dominique's op-ed piece, published by the World Economic Forum as a part of its most recent Davos annual agenda lays out the necessity for these discussions at the leadership level. The article is linked here: How attention to privacy will stabilize our markets (World Economic Forum May 25, 2022).

160

Countries with data protection laws located in the regions we have offices

Regulatory Focus on the Board's Duty of Care and Oversight Has Heightened over the Past Year

Recent Developments: FTC April 8, 2021 Report

Corporate boards: Don't underestimate your role in data security oversight

- April 8, 2021, the FTC published *Corporate boards: Don't underestimate your role in data security oversight*.
- In that document, the FTC called for boards to "build a team of stakeholders" who can "...bring a different perspective to the issues."
- The FTC called for the team that reports to the board to include nontechnical leaders such as the CEO, CFO and legal counsel.
- FTC also encouraged boards to review their committee structure to ensure that board oversight over cybersecurity occurs either at the audit committee level or via a standalone committee devoted to cybersecurity
- The FTC called for regular briefings to include privacy and cyber

"When it comes to security, board members need to be in the know, but research suggests many of them are out of the loop."

Privacy Has Cost Companies Trillions in Market Cap

- In 2022, because 85% consumers opted out of mobile tracking due to privacy, NASDAQ listed companies lost $1.4 trillion in market cap. See, *Data Privacy: A Business Imperative for Boards & Leaders That May Contribute to Market Recovery* (NASDAQ, 2022);
- GDPR fines now levied against 1186 companies totaling €2,040,213,207, including:
  - An American multinational technology company focusing on e-commerce, cloud computing, online advertising, digital streaming, and artificial intelligence had the largest GDPR fine of €746,000,000;
  - A global social network was fined €405,000,000;
  - A global cloud provider was fined €90,000,000
- FTC has fined a major micro blogging company $150 million in 2022

Privacy Issues Have Resulted in Over $1.4 Trillion Losses for NASDAQ Listed Companies

Boards and CEOs of Privately Held Companies Must Focus on Data Leadership

- Investors send privacy/data security maturity questionnaires prior to investing.
- Significant **investors** have engaged with companies around cyber and privacy
  BlackRock.com | Investment Stewardship Report: Americas Q1 2018
- Stock exchanges are focusing on data privacy and security.

Recent Developments: NY DFS July 29, 2022 Proposal

Cybersecurity Requirements for Financial Services Companies

- NY DFS' proposed rule would require board approval of cybersecurity policies that cover (at a minimum): "(a) information **security**; (b) **data governance** and classification; and…customer **privacy**."
- "The board or an appropriate committee of **the board shall have sufficient expertise and knowledge, or be advised by persons with sufficient expertise and knowledge,** to exercise effective oversight of cyber risk and a committee or subcommittee assigned responsibility for cybersecurity."

Regulators Recommend Third Party Advisors to Protect the BoD.

Recent Developments: SEC Feb. 9, 2022 Proposed Rule

Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies

- "Proposed rule 38a-2 would require a fund's **board of directors**, including a majority of its independent directors, initially to **approve the fund's cybersecurity policies and procedures**, as well as to review the written report on cybersecurity incidents and material changes to the fund's cybersecurity policies and procedures that…would be required to be prepared at least annually"

- The required written reports… would provide fund directors with **information necessary to ask questions and seek relevant information regarding the effectiveness of the program and its implementation**, and whether the fund has adequate resources with respect to cybersecurity matters, including access to cybersecurity expertise. **We anticipate that a fund's board's review of the written reports would naturally involve inquiries about cybersecurity risks** arising from the program and any incidents that have occurred

"Board oversight should not be a passive activity."

- SEC February 9, 2022 Report

Recent Developments: SEC March 2022 Proposed Rule

Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

- "Cybersecurity is already among the top priorities of many boards of directors [citation omitted] and cybersecurity incidents and other risks are considered one of the largest threats to companies.[Citation omitted] **Accordingly, investors may find disclosure of whether any board members have cybersecurity expertise to be important as they consider their investment in the registrant as well as their votes on the election of directors of the registrant**."

For all public companies, the SEC describes its intention to require disclosure from public companies regarding whether their boards have members with cybersecurity experience.

New Cybersecurity Rules Expected April 2023

FORBES > MONEY > MARKETS

SEC New Rules And Regulations

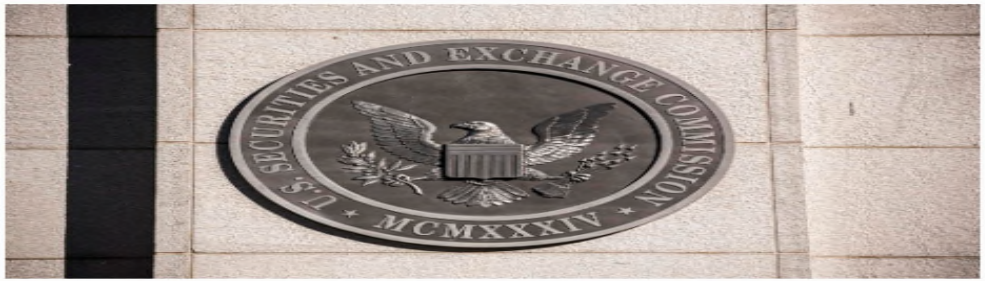
Betsy Atkins Contributor ⓘ
I'm a board vet writing about corporate governance & business trends

Follow

0

Jan 26, 2023, 11:11am EST

Listen to article 14 minutes



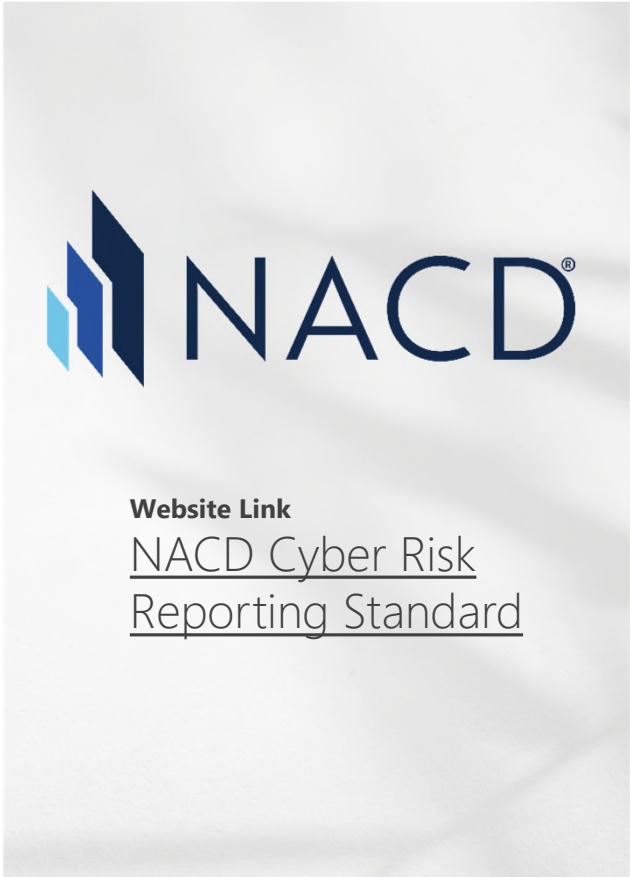
Washington Dc: US Securities and Exchange Commission building exterior. The U.S. Securities and ... [+] GETTY

Welcome to new board oversight duties...It is one of the great things about board work...it is ever changing and evolving. Every year there is a shift in corporate governance standards in an effort to evolve along with the rapidly changing business landscape and stay aligned with the

Proposed Action: Focus on Financial Metrics

Board reports should highlight the financial exposure attributed to the organization's cyber risk leveraging the same analytics used by leaders within the cyber insurance industry. The board reports should include:

- An organization's overall financial exposure to cyber risks and cyber-attacks,
- A view of the cyber threats most likely to cause financial losses to a business,
- Insights on the cyber controls/investments most effective in mitigating financial losses, and
- Insights on cyber risk transfer/cyber insurance, including "stress testing" existing policies across a range of potential cyber incidents.



Shareholder Derivative Actions Naming BoD Re Privacy & Cyber are on the Rise – Over 75 Actions filed

CPO MAGAZINE HOME NEWS INSIGHTS RESOURCES

In recent months, a trend has begun to emerge among plaintiffs' lawyers seeking to file cybersecurity incident-related shareholder derivative lawsuits – attorneys are increasingly now filing claims specifically based on failures surrounding duty of oversight. In November of 2021, a shareholder derivative lawsuit was filed against T-Mobile USA's board of directors, pointing to a lack of monitoring and acting upon obvious red flags. Kevin M. Lacroix excellently outlines this trend in The D&O Diary. Directors should take notice.

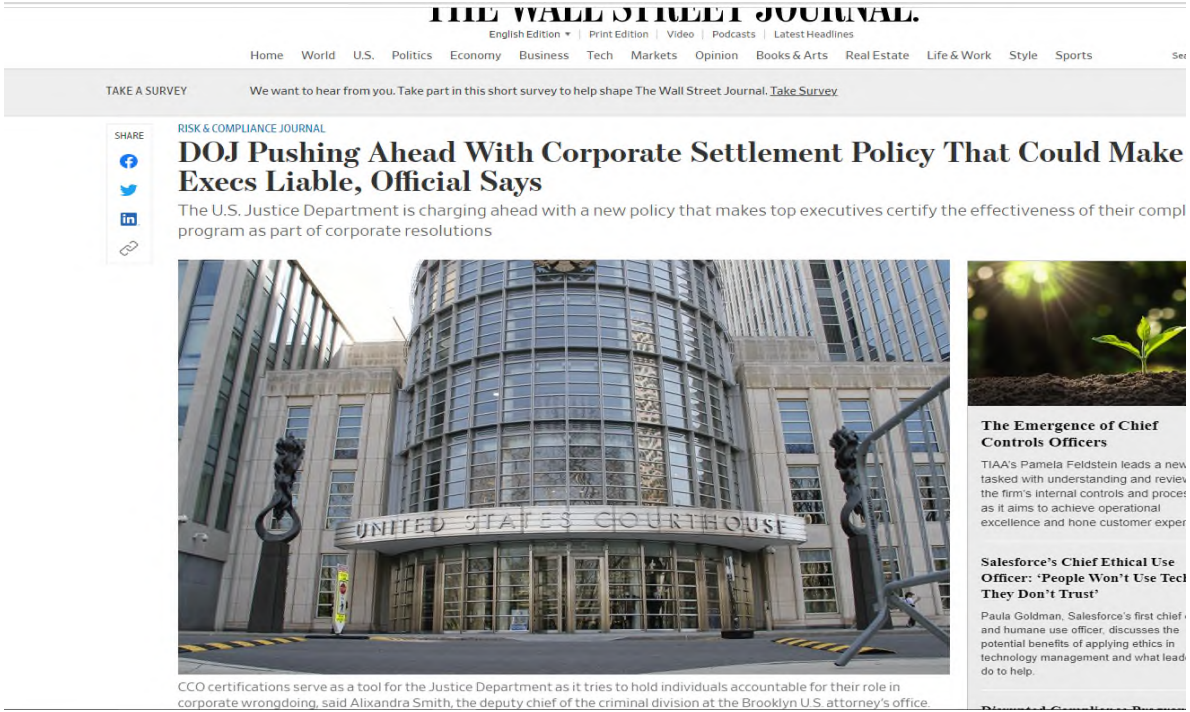
Mayer Brown has identified over 75+ shareholder derivative actions pertaining to privacy and cyber.

Triggering Conduct for BoD liability

United States

1. Failure to Stay Informed
2. Lack of a Board Committee with Data Privacy and Security Oversight
3. Lack of Qualified Officers
4. Failure to Safeguard Personal Data
5. Failure to Respond to Known Cyber Threats
6. Failing to Conduct Adequate Due Diligence
7. False SEC Filings and Other Public Statements
8. Lack of Transparency
9. Insufficient Oversight of Vendors and Third Parties
10. Failure to Provide Timely and Adequate Notices
11. Compliance with Laws

DOJ's New Stance on Corporate Enforcement



THE WALL STREET JOURNAL.

English Edition | Print Edition | Video | Podcasts | Latest Headlines

Home World U.S. Politics Economy Business Tech Markets Opinion Books & Arts Real Estate Life & Work Style Sports

TAKE A SURVEY We want to hear from you. Take part in this short survey to help shape The Wall Street Journal. Take Survey

SHARE

RISK & COMPLIANCE JOURNAL

DOJ Pushing Ahead With Corporate Settlement Policy That Could Make Execs Liable, Official Says

The U.S. Justice Department is charging ahead with a new policy that makes top executives certify the effectiveness of their compl program as part of corporate resolutions

CCO certifications serve as a tool for the Justice Department as it tries to hold individuals accountable for their role in corporate wrongdoing, said Alixandra Smith, the deputy chief of the criminal division at the Brooklyn U.S. attorney's office.

The Emergence of Chief Controls Officers

TIAA's Pamela Feldstein leads a new tasked with understanding and revie the firm's internal controls and proce as it aims to achieve operational excellence and hone customer exper

Salesforce's Chief Ethical Use Officer: 'People Won't Use Tech They Don't Trust'

Paula Goldman, Salesforce's first chief and humane use officer, discusses the potential benefits of applying ethics in technology management and what lead do to help.

"The U.S. Justice Department isn't backing away from a policy, criticized by some in the corporate sector, of having compliance officers sign off on the effectiveness of their programs as part of settlements.

The certifications serve as a tool for the Justice Department as it tries to hold individuals accountable for their role in corporate wrongdoing, said Alixandra Smith, the deputy chief of the criminal division at the Brooklyn U.S. attorney's office."

***Wall Street Journal*, September 22, 2022**

Article Link

DOJ Pushing Ahead With Corporate Settlement Policy That Could Make Execs Liable, Official Says

Global Focus on BoD Oversight of Privacy & Cyber

- **EU** draft Digital Operational Resilience Act (DORA) covers financial services, crypto, payments and others. DORA states: "Members of the management body shall, on a regular basis, follow specific training to gain and keep up to date sufficient knowledge and skills to understand and assess **[Information Communication Technology]** ICT risks and their impact on the operations of the financial entity." NIST 2 – focus on "managing bodies" accountability. Draft Artificial Intelligence Act.

- The **United Kingdom's** National Cyber Security Centre (NCSC) has a Cyber Security Toolkit for Boards website that contains "[r]esources designed to encourage essential cyber security discussions between the Board and their technical experts."

- **Denmark** guidance emphasizes BoD's oversight role when it comes to cyber Centre for Cyber Security (CFCS) published a December 2019 cybersecurity guidance for boards of directors.

- **Australian Securities & Investment Commission** counseled board members to ask themselves: "**Does the board need further expertise to understand the risk?** Although boards may not require general technology expertise, for many companies it may be advisable to have one or more directors who have a strategic understanding of technology and its associated risks, or who have a background in cybersecurity. In some circumstances, *the board should consider the use of external cyber experts to review and challenge the information presented by senior management.*

BoD is the focus of regulators in the EU, MEA, and APEC.

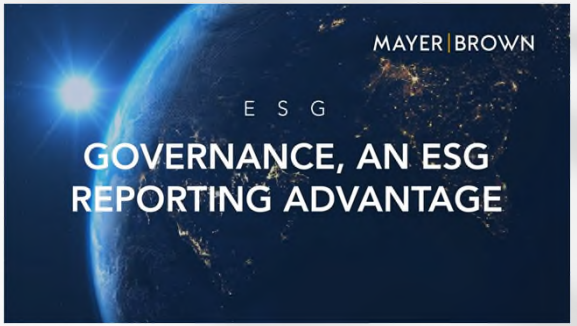
Privacy & Cyber Are Measured Under the Governance Prong of ESG

GLOBAL DATA INNOVATION PRACTICE

Privacy & Cyber Are Being Rated as Part of ESG by Proxy Advisors and Investors

- Institutional Shareholder Services ("**ISS**") rates companies on their cyber and privacy practices via the governance prong of and issues a Cyber Risk Score
  ISS Governance.com | ESG Cyber Risk Score™
- Global Reporting Initiative (**GRI**), relied on for ESG reporting by many companies, has issued a specific
  "Customer Privacy Standard"
- Significant **investors** have engaged with companies around cyber and privacy
  BlackRock.com | Investment Stewardship Report: Americas Q1 2018

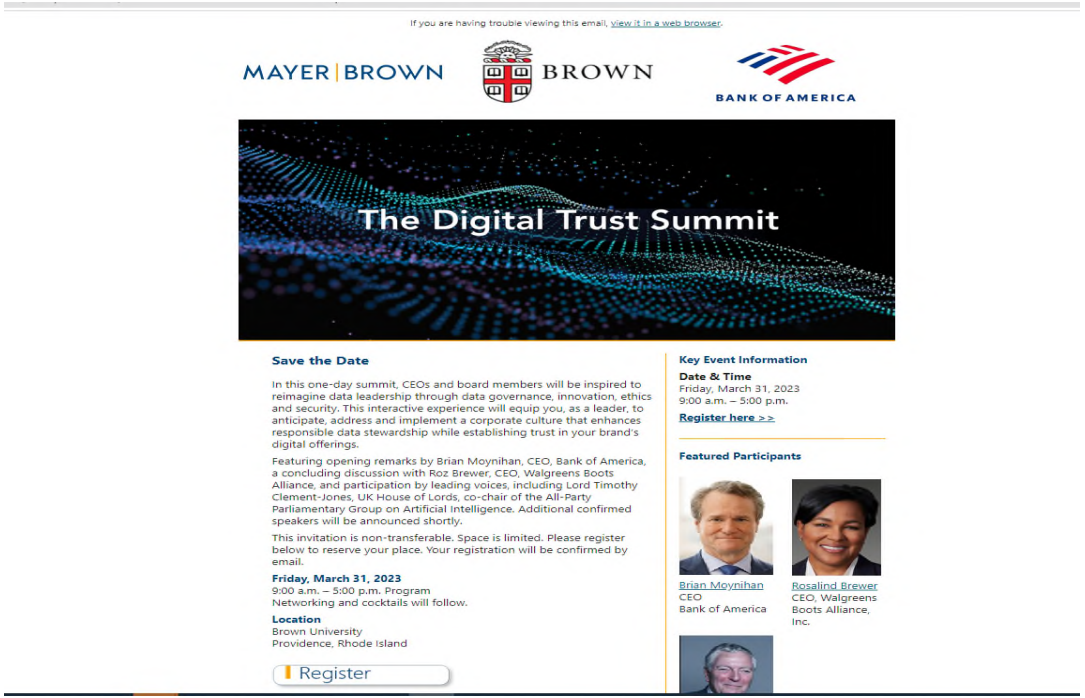
Video



Website Link

Critical Privacy Elements in ESG Scoring

Digital Trust Summit



If you are having trouble viewing this email, view it in a web browser.

MAYER | BROWN BROWN BANK OF AMERICA

The Digital Trust Summit

Save the Date

In this one-day summit, CEOs and board members will be inspired to reimagine data leadership through data governance, innovation, ethics and security. This interactive experience will equip you, as a leader, to anticipate, address and implement a corporate culture that enhances responsible data stewardship while establishing trust in your brand's digital offerings.

Featuring opening remarks by Brian Moynihan, CEO, Bank of America, a concluding discussion with Roz Brewer, CEO, Walgreens Boots Alliance, and participation by leading voices, including Lord Timothy Clement-Jones, UK House of Lords, co-chair of the All-Party Parliamentary Group on Artificial Intelligence. Additional confirmed speakers will be announced shortly.

This invitation is non-transferable. Space is limited. Please register below to reserve your place. Your registration will be confirmed by email.

Friday, March 31, 2023
9:00 a.m. – 5:00 p.m. Program
Networking and cocktails will follow.

Location
Brown University
Providence, Rhode Island

Register

Key Event Information

Date & Time
Friday, March 31, 2023
9:00 a.m. – 5:00 p.m.

Register here >>

Featured Participants

Brian Moynihan
CEO
Bank of America

Rosalind Brewer
CEO, Walgreens Boots Alliance, Inc.

Thank you, Questions & Resources

CYBERSECURITY & DATA PRIVACY

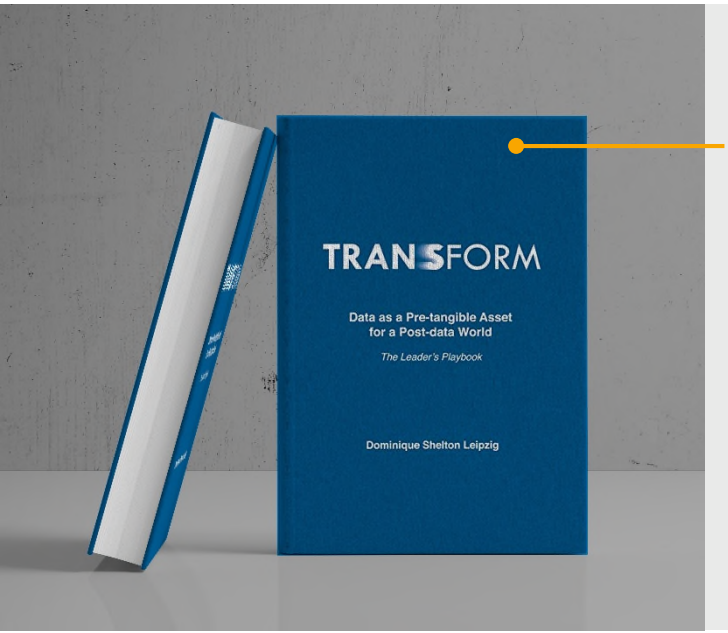
Rajesh De
Partner, Washington DC
rde@mayerbrown.com
+1 202 263 3366

Raj De serves on Mayer Brown's global Management Committee. He was previously the Managing Partner of Mayer Brown's Washington DC office, which is comprised of more than two hundred lawyers. He leads the firm's global Cybersecurity & Data Privacy practice, as well as the firm's National Security practice, and serves as a member of the firm's Congressional Investigations & Crisis Management team. After nearly two decades in private practice and public service across all three branches of the United States government, Raj is one of the most trusted voices in Washington. He has held senior appointments in the White House, the Department of Justice (DOJ) and the Department of Defense (DOD). Raj returned to Mayer Brown in 2015 after serving as General Counsel at the United States National Security Agency (NSA). Since returning to the firm, Raj has received numerous recognitions, including by American Lawyer ("Lateral All-Star"), Washingtonian magazine ("Top Lawyer"), The National Law Journal ("Cybersecurity and Data Privacy Trailblazer"), and Cybersecurity Docket ("Incident Response 30").

Dominique Shelton Leipzig
Partner, Los Angeles
dsheltonleipzig@mayerbrown.com
+1 312 701 8623

Dominique is the lead for the Global Data Innovation as well as Ad Tech Privacy & Data Management practices. She is one of the country's top privacy and data lawyers, and her considerable experience helps clients navigate the evolving legal compliance issues related to privacy and data security for their digital data initiatives. Among her many accolades, Dominique has been named to the "Top 100 Women Lawyers in California" by The Daily Journal (2021); a "Woman of Influence" by The Los Angeles Business Journal (2021); and an "Incident Response 40" by the Cybersecurity Docket (2019–2022). She is also ranked in both Chambers Global (2021-2022) and Chambers USA (2020-2022) for Privacy & Data Security. Dominique is co-founder and co-CEO of NxtWork and has been appointed to the Nasdaq Center for Board Excellence's Risks and Cybersecurity Insights Council.

Resources



BY DOMINIQUE SHELTON LEIPZIG:

Transform - Data as a Pre-tangible Asset for a Post-data World

Today every company is a data company – because every company needs data to grow, thrive, and develop now and into the future.

MAYER BROWN PUBLICATIONS:

Resilience Requires a Modern Path to Board-Level Cyber, Privacy and Data Risk Governance

5 Steps for the Boardroom Community to Address Heightened Privacy and Cyber Risk Oversight

Americas | Asia | Europe | Middle East

mayerbrown.com