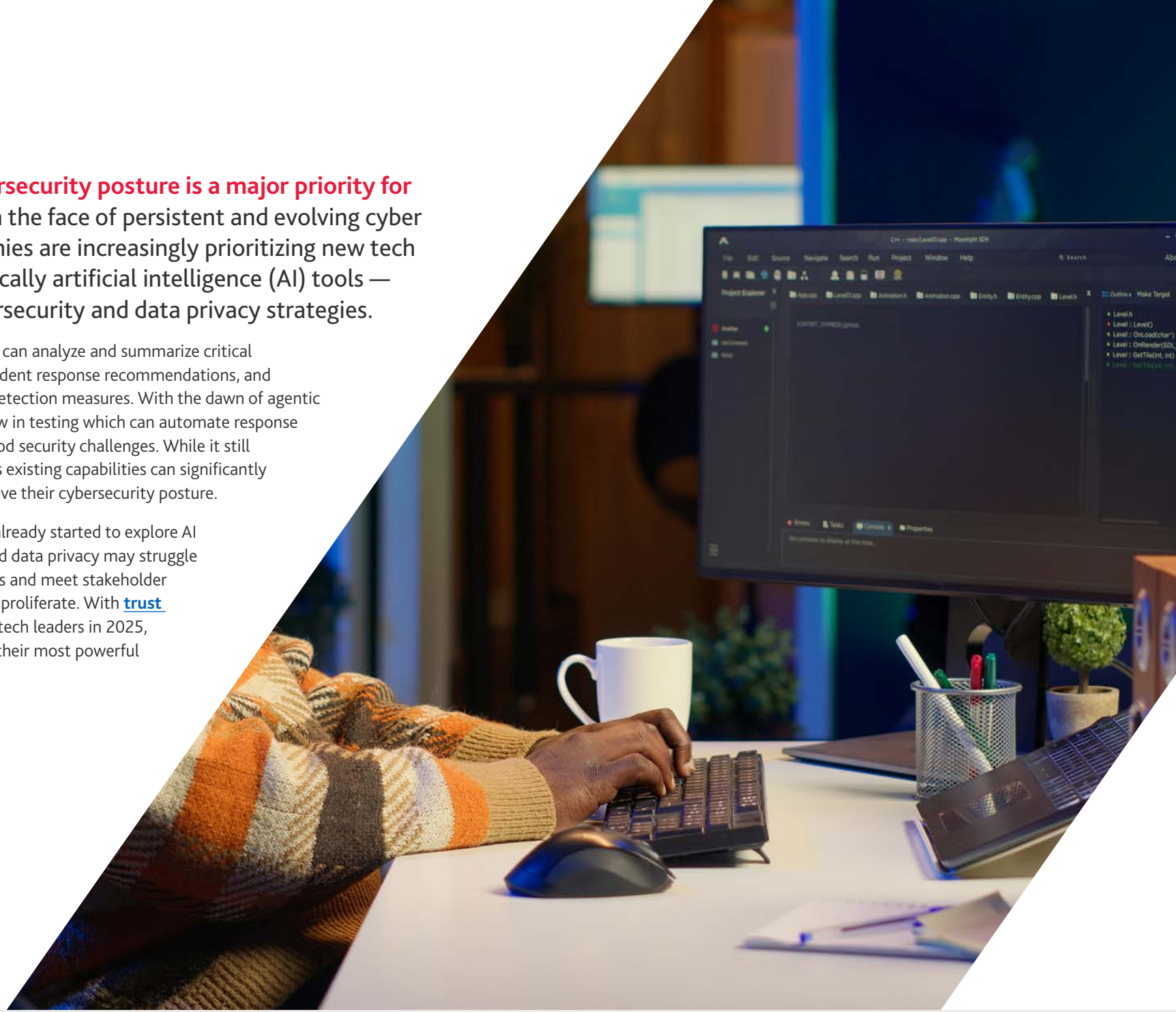
# AI
# Tech's Key to Cybersecurity Resilience

BDO

**Strengthening cybersecurity posture is a major priority for the tech industry.** In the face of persistent and evolving cyber threats, tech companies are increasingly prioritizing new tech integration — specifically artificial intelligence (AI) tools — to bolster their cybersecurity and data privacy strategies.

Among its many use cases, AI can analyze and summarize critical documentation, generate incident response recommendations, and implement real-time threat detection measures. With the dawn of agentic AI, cybersecurity tools are now in testing which can automate response tasks based on well-understood security challenges. While it still requires human oversight, AI's existing capabilities can significantly help tech organizations improve their cybersecurity posture.

Organizations that have not already started to explore AI solutions for cybersecurity and data privacy may struggle to keep pace with competitors and meet stakeholder expectations as cyber threats proliferate. With **trust and security** top of mind for tech leaders in 2025, they should not leave one of their most powerful tools on the table.



# Understanding the Urgency

Microsoft's latest **Digital Defense Report** reveals that its customers face an average of 600 million cyberattacks each day. These rates are too high for even the most skilled cybersecurity leaders to sustain. AI can significantly help tech companies — especially middle market companies with fewer resources than their larger peers — keep pace with the growing volume of threats they face.

AI can also help companies maintain compliance with an evolving landscape of cybersecurity laws and regulations. In 2023, the SEC **adopted rules** on cybersecurity risk management, strategy, governance, and incident disclosure. Organizations are now required to disclose any material cybersecurity incident in a shorter timeframe than ever before. In addition to the SEC rules, 42 individual states have adopted their own data privacy regulations, potentially making it more difficult for tech companies to comply. Tech companies can use AI to rapidly gather the necessary information to support required data privacy disclosures, summarize or integrate data from across systems to build regulatory reports and views, as well as analyze state-specific rules and summarize reporting needs.

# AI Use Cases in Cybersecurity and Data Protection

AI offers a range of use cases to help strengthen an organization's data privacy and cybersecurity processes. Some are quicker to implement while others are still emerging and may require more time and resources to execute.

1. **Layering Generative AI into a Security Program:** Generative AI can quickly analyze, summarize, and document critical information about a breach incident and recommend triage responses. This use case, while straightforward, is one of the most impactful. Security teams can also ask questions about the incident, and AI can provide answers with speed and precision. This information can then be used to support any required disclosures, improve existing policies and procedures, and even serve as a teaching tool to close employee skill gaps.
2. **Prioritize Signals**: AI tooling can use risk signals from many sources to make recommendations around which alerts, events, or indicators need prioritized attention from a human operator. These alert triage tools speed up threat response in "today" toolsets, delivering immediate impact to a security operations teams' risk management and response capabilities.
3. **Policy and Regulatory Benchmark Analysis:** AI can scan cybersecurity frameworks and standards and use them as a benchmark to evaluate an organization's own practices. With an enhanced view provided by AI insights, companies can quickly identify security control gaps and opportunities to improve the organization's cybersecurity posture and compliance readiness.
4. **Threat Detection and Behavior Analysis:** AI can help determine the likelihood of a data breach or exposure. For example, it can be programmed to monitor inbound emails and flag potentially dangerous activity. Once the AI is fully trained, the security team can set parameters that allow the AI to flag items of concern — such as an employee engaging with a phishing scam — for review and verification by a team member. AI-powered threat detection can cut the time to identify a threat down to mere seconds, as opposed to hours, days, weeks, or even months.

## THE NEXT PHASE: SECURITY AUTOMATION

While fully autonomous, end-to-end cybersecurity programs have not yet arrived, they represent the next phase of AI integration. Agentic AI can engage in more complex decision making and act independently in the event of a breach. As with AI in other domains, fully automated security programs will free up human time and resources for areas that require even deeper judgement.

There are still challenges to overcome before this function can be realized, particularly around verifying the accuracy of an AI's decisions. In the example of an employee clicking a phishing link in an email, an autonomous AI's remediation strategy might be to wipe that employee's laptop. While it may indeed be necessary in some cases, this response should only be a last resort given the cost expenditure and risk of losing critical information. For now, human oversight remains necessary to guard against a potentially disproportionate AI-driven response.

# How to Prioritize Use Cases and Calculate ROI

A strong cybersecurity and data protection program rests on three core pillars: trust, consistency, and repeatability. AI can be a powerful tool to support these pillars, but as AI becomes more complex and autonomous, tech companies will also need to invest time and resources in evaluating its outputs and its bottom-line impacts.

Understanding potential AI use cases is just one piece of the puzzle. Organizations need a clear implementation plan that identifies priority integration areas and establishes metrics to determine return on investment (ROI), as well as a **strong data governance** framework to support AI enablement.

To effectively prioritize integration areas, companies should first assess where their data infrastructure is currently able to support AI and where it may need improvements.

They should also establish benchmarks for data quality and refinement, as well as develop policies that define acceptable data uses. Companies can then decide which AI use cases to test, in conjunction with their strategic needs.

Once their data foundation is set, organizations may opt to begin AI experimentation with a productized pilot — a ready-made, off-the-shelf solution that teams can start using quickly. If the pilot demonstrates value, they may decide to move up to customized prompts or even to dedicated tooling — solutions that are designed to fit within the business's specific systems. In choosing between these options, the ultimate question tech leaders should ask is: What is the most cost-effective way to enable our cybersecurity professionals?

## PROMPT WRITING FOR CYBER TEAM ENABLEMENT

Quality prompts can help organizations more quickly validate the effectiveness and utility of AI tools. A strong prompt should begin with the end goal in mind, specifying the desired output from the AI tooling — which the rest of the prompt will then support. After stating the goal, set the stage by adding context and detail about what the prompt aims to accomplish, with a focus on the audience, point of view, and other relevant factors. Next, define any parameters. These may be specific sources, samples, or key pieces of data that the AI tooling should engage. Finally, tailor the delivery, stating any expectations for how the AI tooling's response should be delivered. Include elements like length, language, format, and any other qualities necessary to make the output useful.

### Example Prompt

Summarize the Microsoft 365 event with ID '1234' in Microsoft Defender XDR to brief IT leadership executives on the event. Focus on an executive-understandable description of the event including:

1. **Event Details**
   Describe the nature of the event, the type of activity, timing, and affected user accounts.
2. **Threat Level**
   Assess the severity of the event and categorize it.
3. **Source and Destination** Identify the source and destination IP addresses, domains, and any associated devices.
4. **Correlated Alerts**
   List any correlated alerts or related events that might indicate a broader threat.
5. **Recommendations**
   Offer actionable recommendations for mitigating the threat and preventing future occurrences. Use concise and non-technical language and a presentation length of 10 minutes.

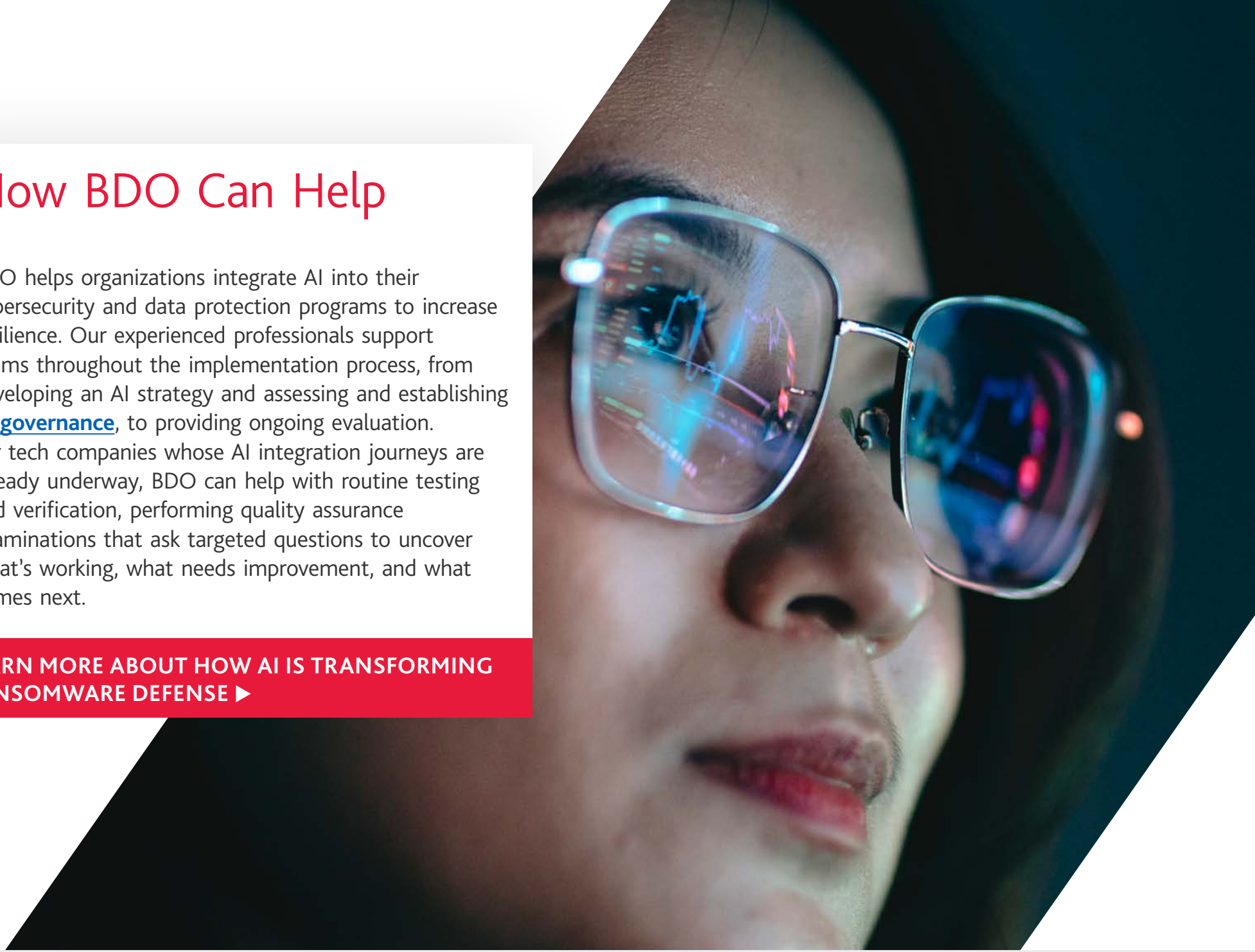
**In tandem with the implementation process, organizations must also be able to demonstrate the ROI of their AI tools. Stakeholders will expect a clear definition of success, and concrete, trackable metrics to measure. For many, the goal of AI integration is to save time — but how much time? And how will that time saved be put to better use? Without answers to these follow-on questions, companies will not be able to fully illustrate the benefits of their AI tools.**

**One approach could be to launch internal assessments that assign specific dollar values to cyber incidents and track the difference before and after AI integration. Then, by comparing a variable — like attacker dwell times before and after integrating AI — companies can tell a clear business story that shows stakeholders the practical and financial benefits of AI.**

# How BDO Can Help

BDO helps organizations integrate AI into their cybersecurity and data protection programs to increase resilience. Our experienced professionals support teams throughout the implementation process, from developing an AI strategy and assessing and establishing **AI governance**, to providing ongoing evaluation. For tech companies whose AI integration journeys are already underway, BDO can help with routine testing and verification, performing quality assurance examinations that ask targeted questions to uncover what's working, what needs improvement, and what comes next.

**LEARN MORE ABOUT HOW AI IS TRANSFORMING RANSOMWARE DEFENSE ▶**



## CONTACT US

**HANK GALLIGAN**
National Technology Industry Leader
hgalligan@bdo.com

**WAYNE ANDERSON**
Director
Cybersecurity
wanderson@bdo.com

**KAREN SCHULER**
Head of Global Privacy & Data Protection
kschuler@bdo.com

Our purpose is helping people thrive, every day. Together, we are focused on delivering exceptional and sustainable outcomes and value for our people, our clients and our communities. BDO is proud to be an ESOP company, reflecting a culture that puts people first. BDO professionals provide assurance, tax and advisory services for a diverse range of clients across the U.S. and in over 160 countries through our global organization.

BDO is the brand name for the BDO network and for each of the BDO Member Firms. BDO USA, P.C., a Virginia professional corporation, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. For more information, please visit: www.bdo.com.