



M&A Insight: A.I. Issues, Climate Change Disclosures & Warranty Insurance

March 28 2024

GIBSON DUNN

MCLE Information

The information in this presentation has been prepared for general informational purposes only. It is not provided in the course of an attorney-client relationship and is not intended to create, and receipt does not constitute, an attorney-client relationship or legal advice or to substitute for obtaining legal advice from an attorney licensed in the appropriate jurisdiction.

- This presentation has been approved for **0.5 General credit**.
- Participants must submit the form by **Thursday, April 4th** in order to receive CLE credit.

CLE Form Link: https://gibsondunn.qualtrics.com/jfe/form/SV_6D5WAekvx9wC97g

Most participants should anticipate receiving their certificate of attendance in 4-6 weeks following the webcast.

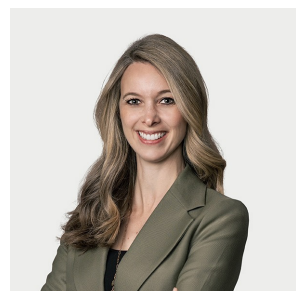
All questions regarding MCLE Information should be directed to CLE@gibsondunn.com.

Today's Panelists



Stephen Glover

[Stephen I. Glover](#) is a partner in the Washington, D.C. office of Gibson, Dunn & Crutcher who has served as Co-Chair of the firm's Global Mergers and Acquisitions Practice. Mr. Glover has an extensive practice representing public and private companies in complex mergers and acquisitions, joint ventures, equity and debt offerings and corporate governance matters. His clients include large public corporations, emerging growth companies and middle market companies in a wide range of industries. He also advises private equity firms, individual investors and others.



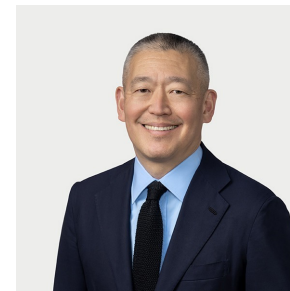
Cassandra Gaedt-Sheckter

[Cassandra Gaedt-Sheckter](#) is a partner in Gibson, Dunn & Crutcher's Palo Alto office, where she co-chairs the global Artificial Intelligence (AI) practice, and is a key member of the Privacy, Cybersecurity and Data Innovation practice, including as the leader of the firm's State Privacy Law Task Force. With extensive experience advising companies on AI, data privacy, and cybersecurity issues, Cassandra focuses on regulatory compliance counseling and privacy and AI program development, regulatory enforcement matters, and transactional representations.



Ahmed Baladi

[Ahmed Baladi](#) is a partner in Gibson, Dunn & Crutcher's Paris office, where he co-chairs the global Privacy, Cybersecurity and Data Innovation practice and is a key member of the AI practice. Ahmed has developed renowned experience in a wide range of privacy and cybersecurity matters including compliance and governance programs in light of the GDPR and other EU Digital Regulations including on AI. He regularly represents companies and corporate executives on investigations and procedures before Data Protection Authorities.



Thomas J. Kim

[Thomas J. Kim](#) is a partner in the Washington D.C. office of Gibson, Dunn & Crutcher, LLP, where he is a member of the firm's Securities Regulation and Corporate Governance Practice Group. Mr. Kim focuses his practice on a broad range of SEC disclosure and regulatory matters, including capital raising and tender offer transactions and shareholder activist situations, as well as corporate governance, environmental social governance and compliance issues. He also advises clients on SEC enforcement investigations – as well as boards of directors and independent board committees on internal investigations – involving disclosure, registration, corporate governance and auditor independence issues.



Jonathan Whalen

[Jonathan Whalen](#) is a partner in the Dallas office of Gibson, Dunn & Crutcher LLP. He is a member of the firm's Mergers and Acquisitions, Capital Markets, Energy and Infrastructure, and Securities Regulation and Corporate Governance practice groups. Mr. Whalen also serves on the Gibson Dunn Hiring Committee. Mr. Whalen's practice focuses on a wide range of corporate and securities transactions, including mergers and acquisitions, private equity investments, and public and private capital markets transactions.

Agenda

01 Introduction

02 SEC's Final Climate Change Disclosure Rules

03 Artificial Intelligence Issues in Acquisition Agreement

04 Developments Update and Warranty Insurance Market

SEC's Final Climate Change Disclosure Rules

SEC's Final Climate Change Disclosure Rules

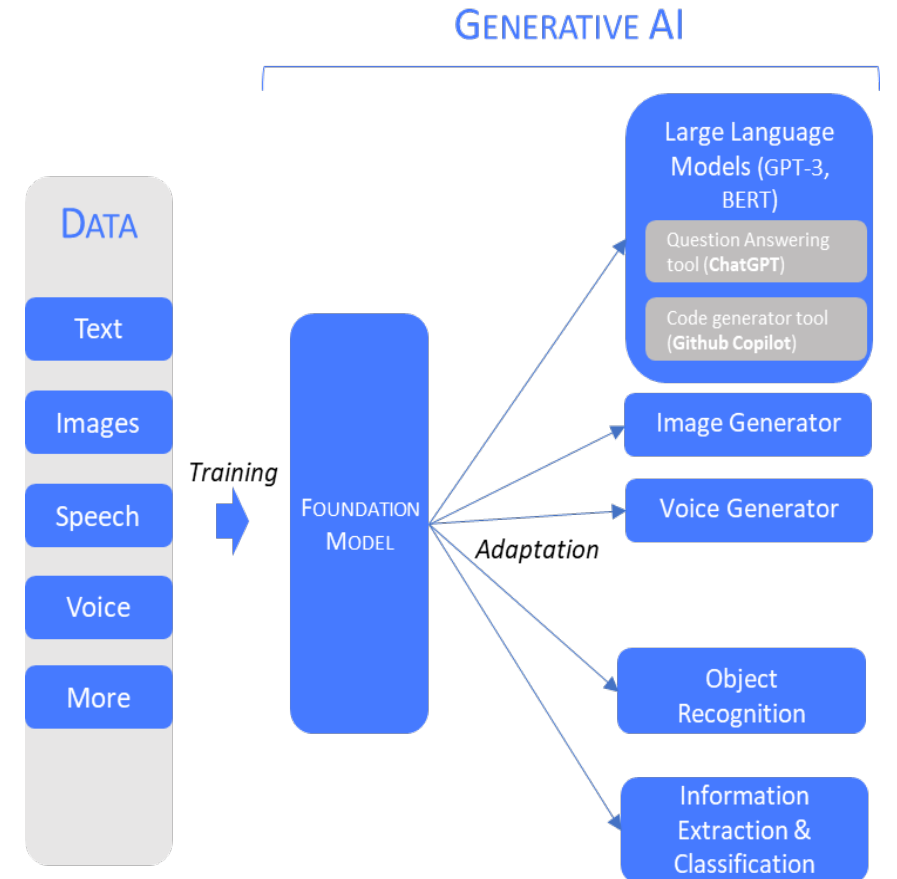
- Proposed SEC climate change disclosures requirements would have applied to private company targets. Specifically, Form S-4, which registers exchange offers, would have required extensive climate risk and governance disclosures, as well as a new financial statement footnote, for private company targets.
- **M&A bar strongly objected.** Public companies could be placed at a competitive disadvantage when bidding to acquire a private company. M&A process would become much more difficult and costly for private companies. Whether to use stock versus cash as merger consideration – this decision would now be impacted by disclosure burden considerations.
- SEC acknowledged these concerns and stated that it did not want to “discourage business combination activity in U.S. public markets.” Accordingly, the SEC determined **not** to require compliance with new climate disclosure requirements for private company targets in Form S-4 or Form F-4.
- **No relief for IPOs.** Private companies looking either to go public or to be acquired will face markedly different compliance burdens as between the two choices.



Artificial Intelligence Issues in Acquisition Agreements

Key Definitions

- **Artificial Intelligence**
 - Capability of a computer system to mimic human cognitive functions such as learning and problem-solving. Through AI, a computer system uses math and logic to simulate the reasoning that people use to learn from new information and make decisions*
- **Machine Learning**
 - Subset of AI which essentially employs advanced statistics in order to construct frameworks with the ability to learn from available data, identify patterns and make **predictions** without requiring human intervention
- **Generative AI**
 - Systems, including **large language models** (LLMs), that process data (visual, textual, audio...), “learn” associations from such data, and generate “new” content (“outputs”) in response to user prompts
- **Foundation Models**
 - AI model pre-trained on large amounts of unlabeled and unsupervised data that can be adapted to many applications/tasks with or without modification and fine-tuning for other, more specialised AI systems
- **Large Language Model**
 - **Foundation models** that are trained on large amounts of text data (to learn patterns and relationships in the language – using neural networks) to process and understand natural language and **predict** and **generate human-like text** (they can be categorized as natural language processing).



*Microsoft

Snapshot Comparison- Regulatory Regimes / Proposals



European Union

- **Single comprehensive legislative framework** in the form of the AI Act.
- **Horizontal** (i.e., cross-sector) and **risk-based** approach to regulating AI.
- Complementary **product liability** regimes being developed.
- Harmonized technical standards to ensure **interoperability**.



Canada

- Draft **Artificial Intelligence and Data Act (AIDA)** inspired by the EU AI Act
- **Horizontal** (i.e., cross-sector approach) and **risk-based** approach to regulating AI



United Kingdom

- **Sectoral approach**: responsibility placed on existing regulators.
- Regulation based on five cross-cutting principles:
 1. safety, security and robustness;
 2. appropriate transparency and explainability;
 3. fairness;
 4. accountability and governance; and
 5. contestability and redress.



United States

- **Cross-sector & sector-specific** regulatory guidance and emergent best practices
- **AI-specific** legislation mainly enacted at state and local level
- Technical **standards** and **benchmarks**
- **Executive Order** on Safe, Secure, and Trustworthy AI



APAC

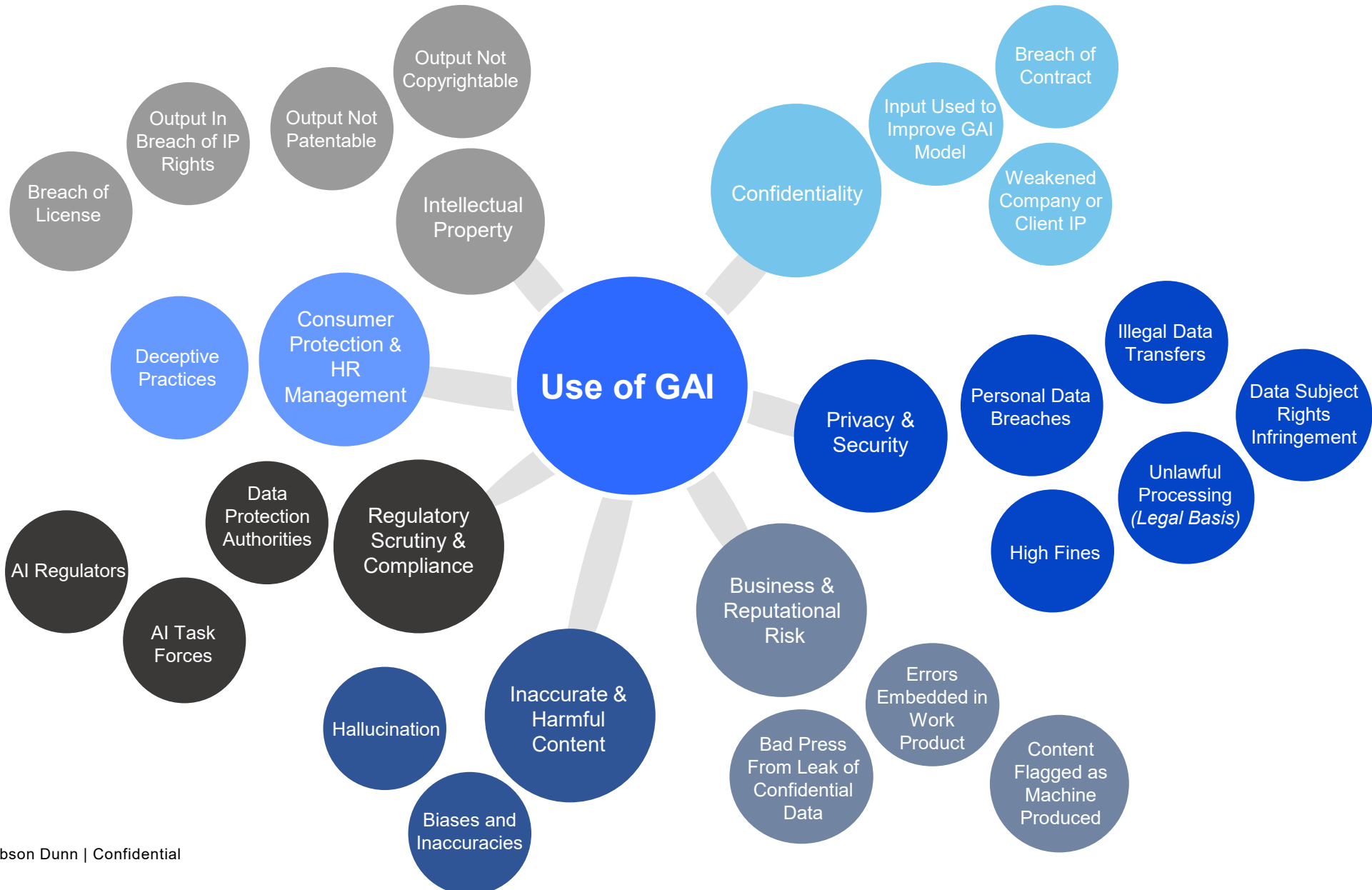
- **Japan: Light touch** approach to AI regulation. Recent regulatory reform has been to promote the development and use of AI.
- **South Korea: Centralised regulation.** Passed the Law on Nurturing the AI Industry and Establishing a Trust Basis in February 2023.
- **Singapore: Light touch** approach with a focus on fostering AI innovation. Instead of legislation, AI best-practice guidelines and an AI testing framework and toolkit (AI Verify).



China

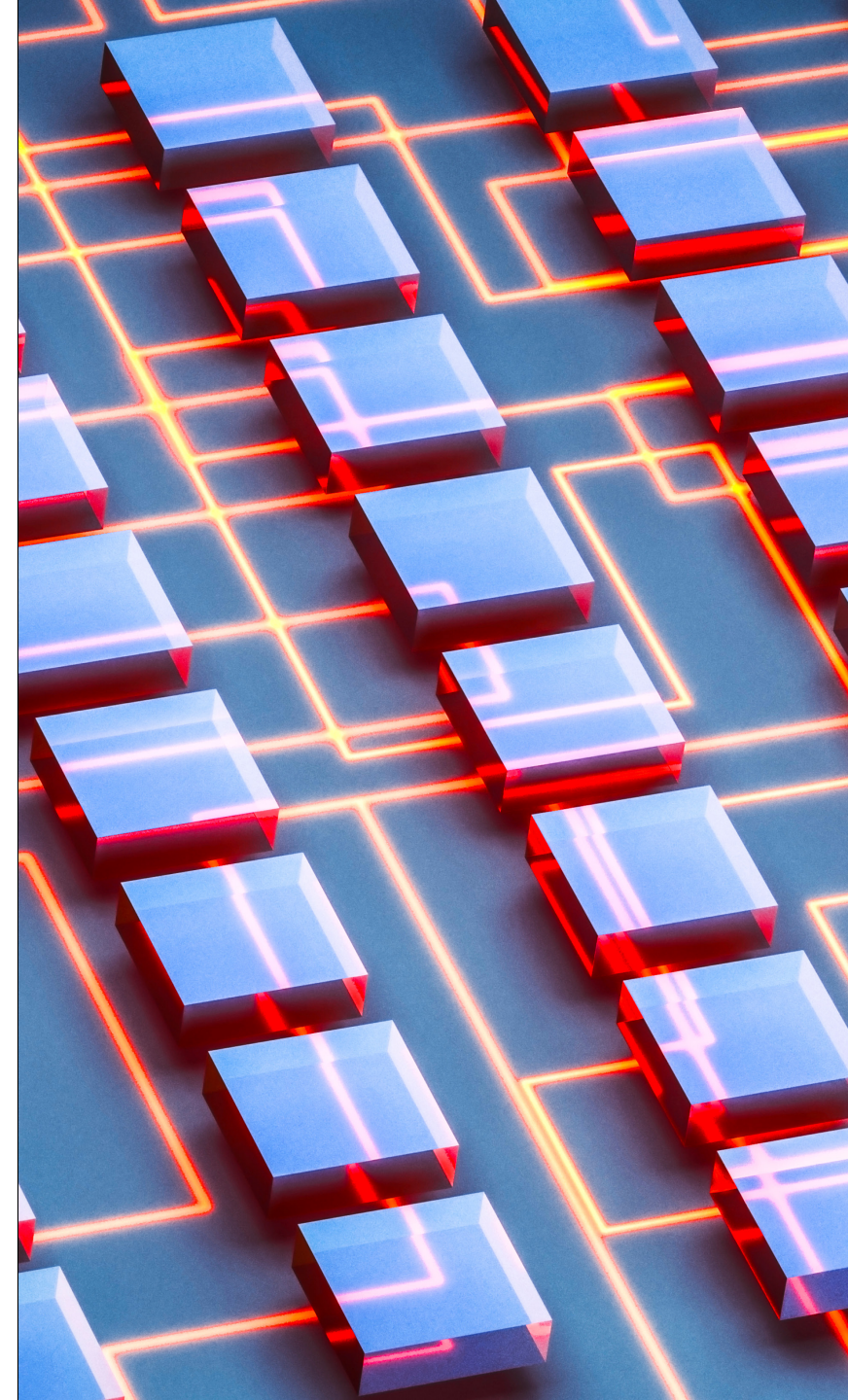
- **Decentralised approach**: regulators responsible for regulation
- The Cyberspace Administration of China's rules regulating Generative AI came into effect in August 2023.
- The "Measures" apply to the **use of generative AI** technologies to provide services to the public in the mainland PRC for the generation of text, images, audio, video, or other content
- A comprehensive **draft AI Law** is expected to be submitted to the legislative body of the PRC sometime in 2024

Generative AI Specific Risks- Risk Mapping



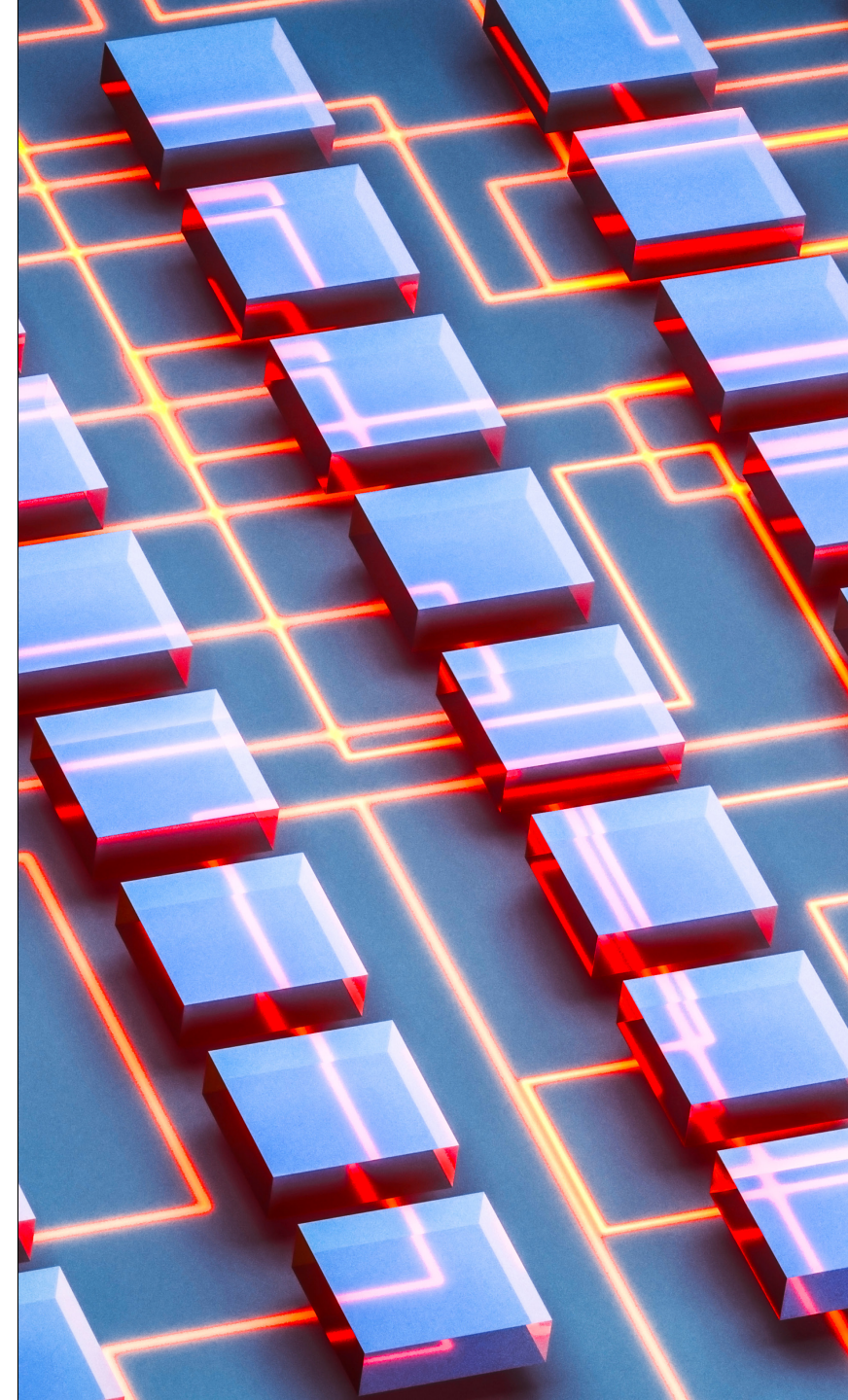
Including AI in M&A Due Diligence

- **AI mapping**- AI systems used or developed
- **Identification of Relevant Applicable AI regulation**- scope of application
- **Classification of the AI system**- AI Act; general purpose, prohibited, high-risk, subject to transparency obligations
- **Training**- input data, web scraping, minimization, automated decision making purpose
- **Output**- verification, copyright, trade secrets, confidentiality, personal data
- **Transparency**- obligations, use of personal data for AI training, data sets used for training, use of copyrighted material to train AI, explainability
- **Data Subjects Rights**- opt out, obtain human intervention, express point of view, obtain explanation of decision reached, contest the decision, consent, right to access, delete etc.
- **Risk Assessment**- DPIA, fundamental rights impact assessment, children data, biometric data
- **Human Oversight and Audit**
- **Dark Patterns and Manipulation**
- **AI Governance**- board, reporting, cross-functional
- **Employee & Staff training**- use of AI systems, processing of personal data for use of AI systems
- **Security Measure**- vulnerabilities
- **Enquiries**, complaints, investigations, claims



Including AI in M&A Agreements

- **Rights to AI Systems**
- **Rights to Data**- training data, input data, output data
- **Use Case Restrictions / Prohibitions**
- **Compliance with Applicable Regulations**- AI, Privacy, Cybersecurity, IP, sector specific
- **Users' Rights**- opt out, obtain human intervention, express point of view, obtain explanation of decision reached, contest the decision, consent, right to access, delete
- **Human Oversight and Audit**
- **Contractual Obligations**- towards developers, vendors, users
- **AI Governance**
- **Security incidents**- vulnerabilities, notification to regulators, claims
- **Enquiries, complaints, investigations, claims?**



Recommendations for AI Usage

1. Usage Policies

- Implement AI system usage policies (including GAI), regular review of such policies and ensure employees approved for the use of such AI systems annually recommit to the internal policy (no input of confidential or personal data, strict assessment of data used to train GAI tools)

2. AI Committee

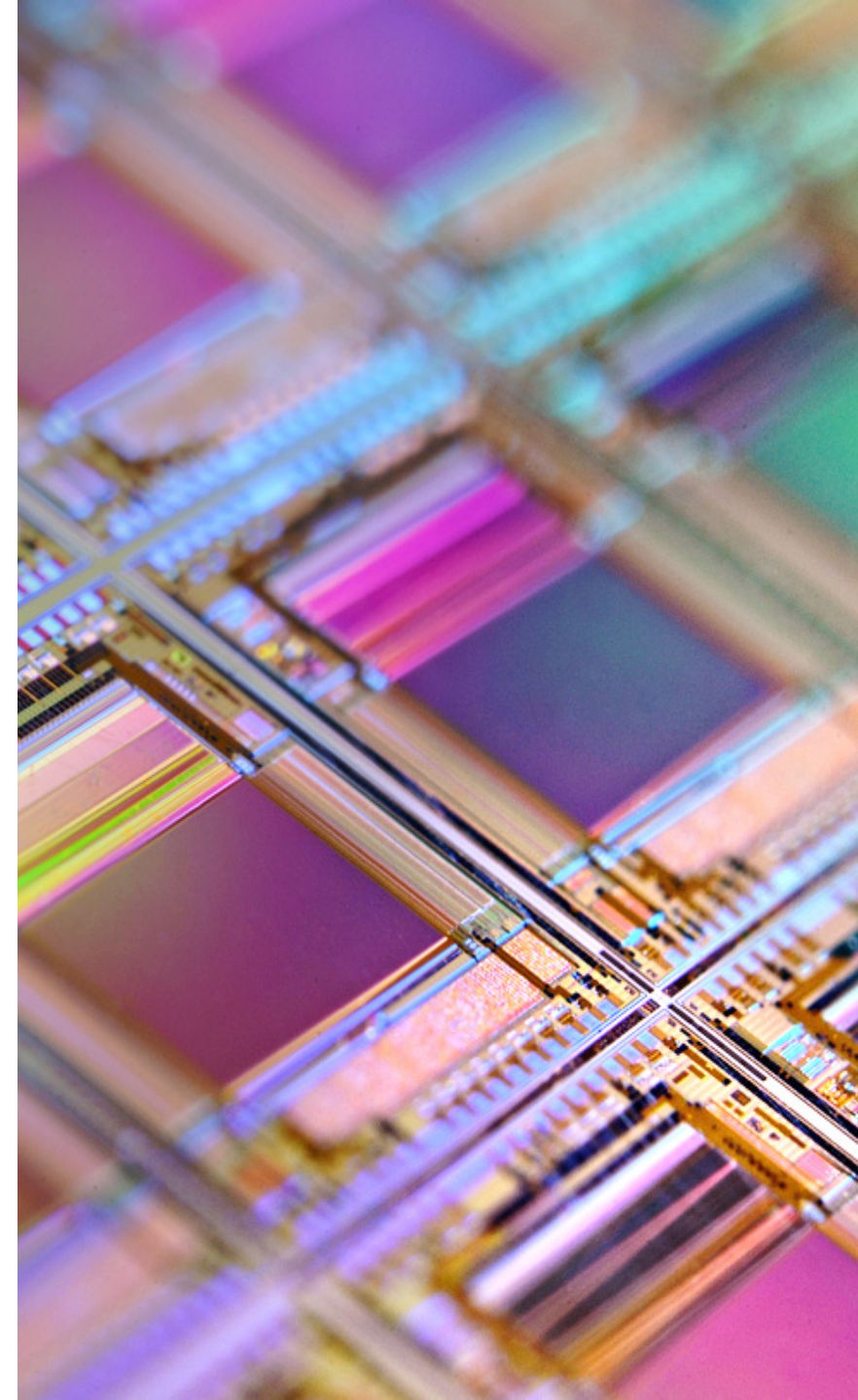
- Create a cross-functional working group/committee to oversee Company's governance efforts, approve requests for use of AI systems and advise the board on AI-related issues

3. Third Party Vendor Oversight

- Implement policies and procedures to address AI risks and benefits arising from third party software and data and other supply chain issues
- Implement third-party vendor assessment and monitoring measures and reduce uncertainty about controller and processor responsibilities regarding the use of AI systems

4. Commonly Used Third Party Systems

- Align usage policies with any existing B2B agreements and licenses, consider any applicable third party terms of use and incorporate these elements in Company's policies



Recommendations for AI Usage

5. Risk Analyses

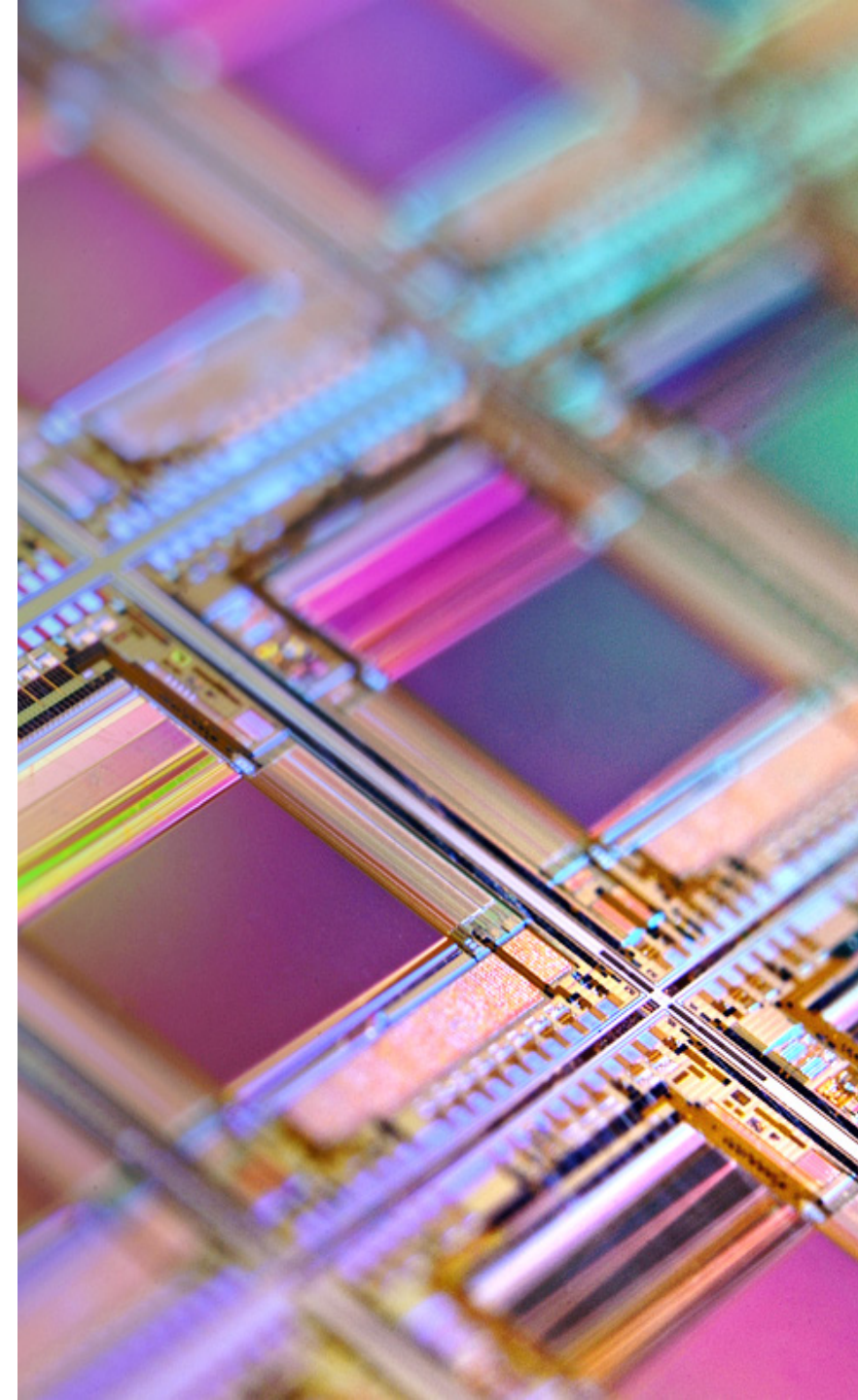
- Conduct use-case-specific risk assessments where appropriate, considering limitations on certain uses subject to authorization from a designated authority. Ensure the use of AI complies with ethical and applicable professional codes and the evolving regulatory framework

6. Restricting Use Cases

- Identify and prohibit certain high risk use cases specific to Company's operations (code generation, product design) that could infringe IP rights and in spell out these prohibitions in internal usage policies

7. Privacy

- Ensure compliance of AI systems with data protection laws
- Review existing policies to inform data subjects of the new personal data processing by AI systems and provide them with an effective way to exercise their right under the GDPR
- Use privacy enhancing technologies (federated learning, differential privacy and secure enclaves) when designing AI systems
- Implement enhanced privacy by design when developing AI systems to ensure compliance with the GDPR principles (establish a clear purpose, legal basis, define a specific retention period, supervise continuous improvement of the AI system, enhanced transparency and explainability of the AI system, ensure data subjects can effectively exercise their rights in the development and operation phase of the AI system)
- The design of AI systems must follow privacy principles, as well as ensure their security, explain ability, fairness and human oversight



Recommendations for AI Usage

8. Quality Control

- Deploy tools to determine whether information was generated by AI systems in violation of Company's policies

9. Usage Tracking

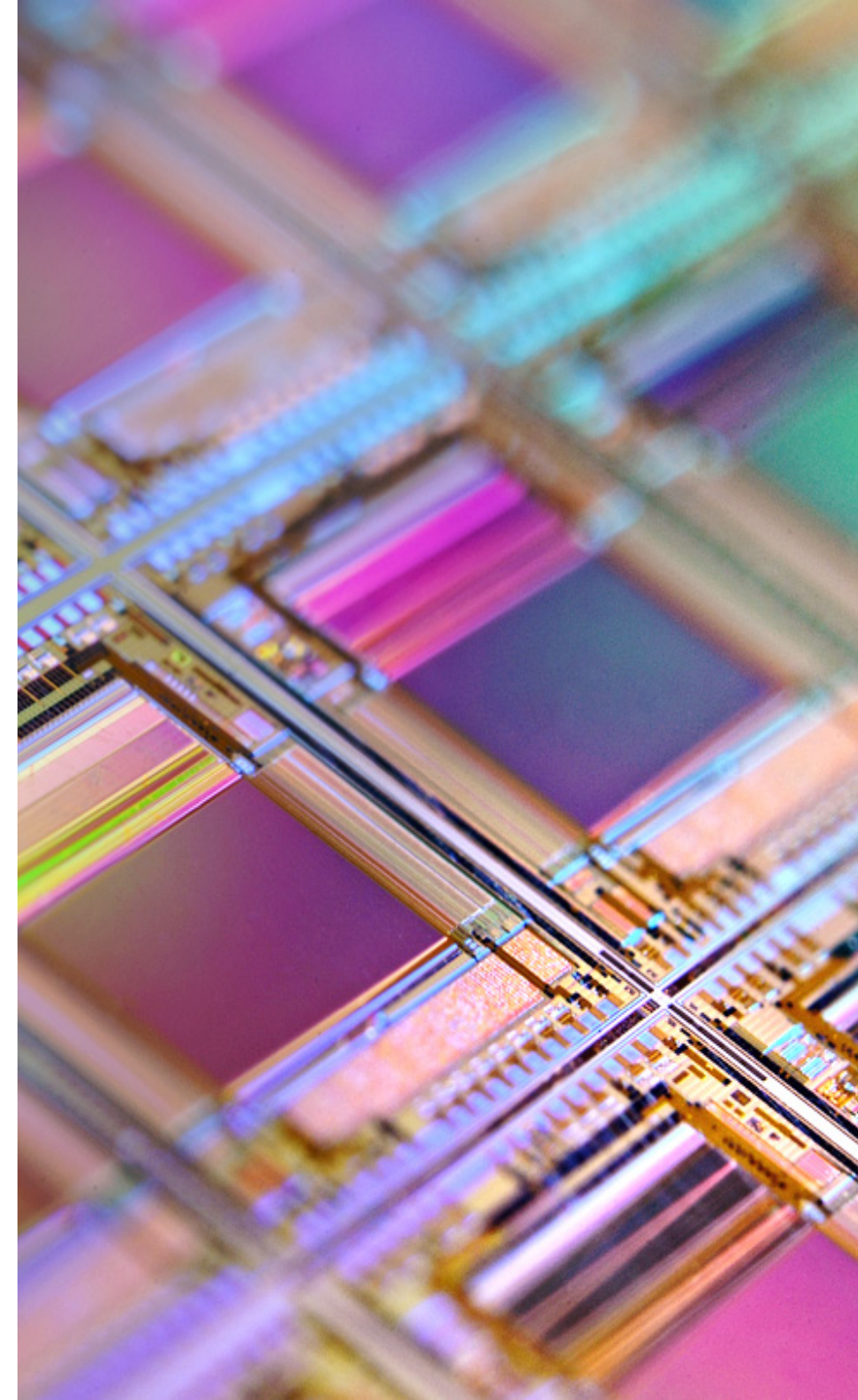
- Teams and employees approved for GAI use should track their usage and report to the GAI Committee to be able to track GAI tools usage and flag issues

10. Monitoring

- Create an internal inventory of GAI tools used and track specific issues and opportunities (implement Company-run GAI tools through APIs or develop proprietary software in the future)

11. Transparency

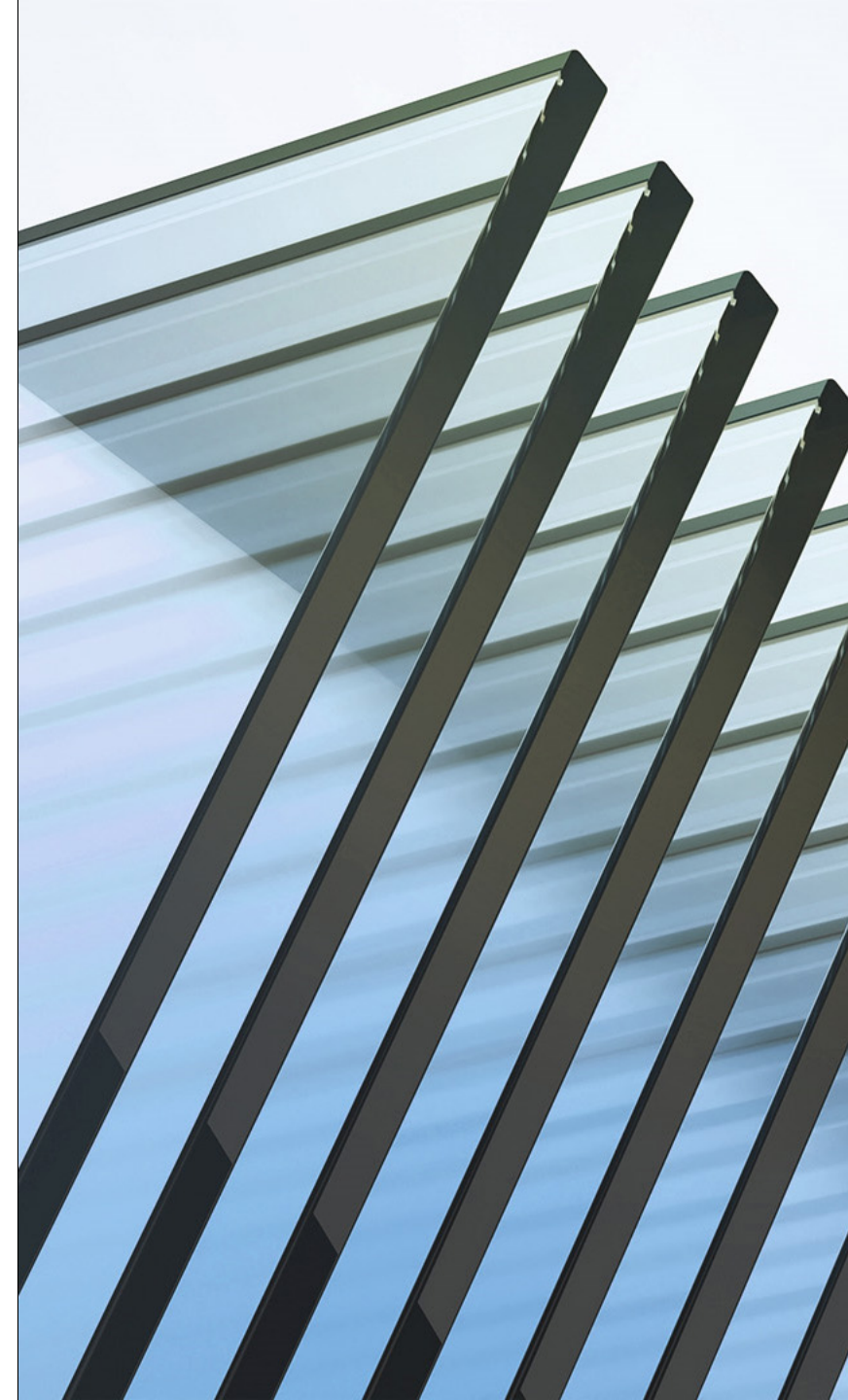
- Ensure teams and employees are aware of the key legal risks, the potential for GAI output to be incorrect and unreliable and the fact that AI generated output can be analyzed to show they are machine-produced



Developments Update & Warranty Insurance Market

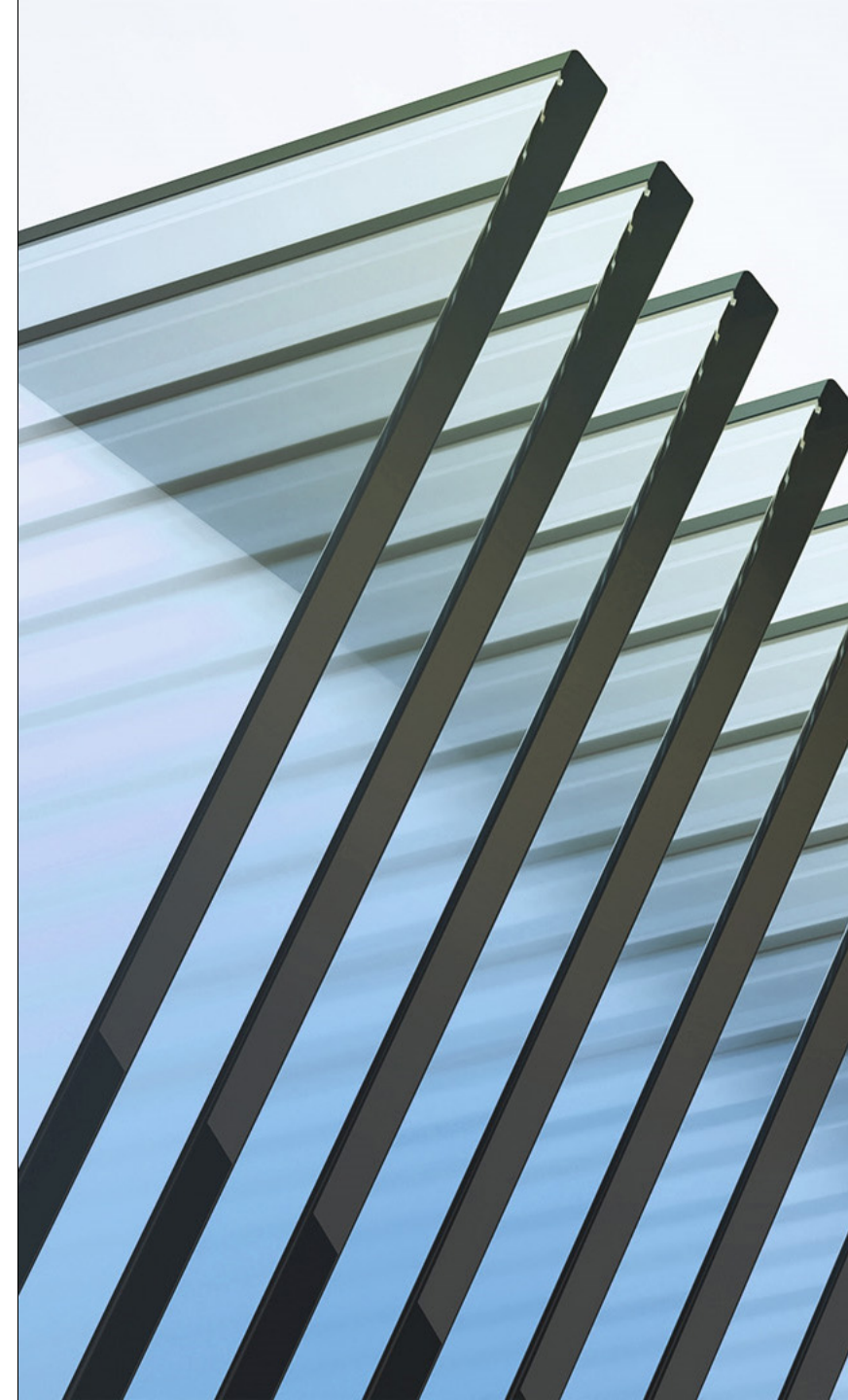
Pricing Trends in Representation & Warranty Insurance

- **Significant Decrease in Premiums:** The market has seen a remarkable decrease in premium rates, hitting historic lows.
- **Substantial Reduction in Retentions:** Since the beginning of 2023, the market has experienced notable drops in both initial and subsequent retention rates, easing entry for smaller deals.
- **Market Competition Intensifies:** The decline in both premiums and retention amounts reflects heightened competition among insurers in an environment of reduced M&A deal flow.
- **Future of Pricing:** With narrowing premium rate variances in late 2023, there's an anticipation of rates potentially stabilizing.



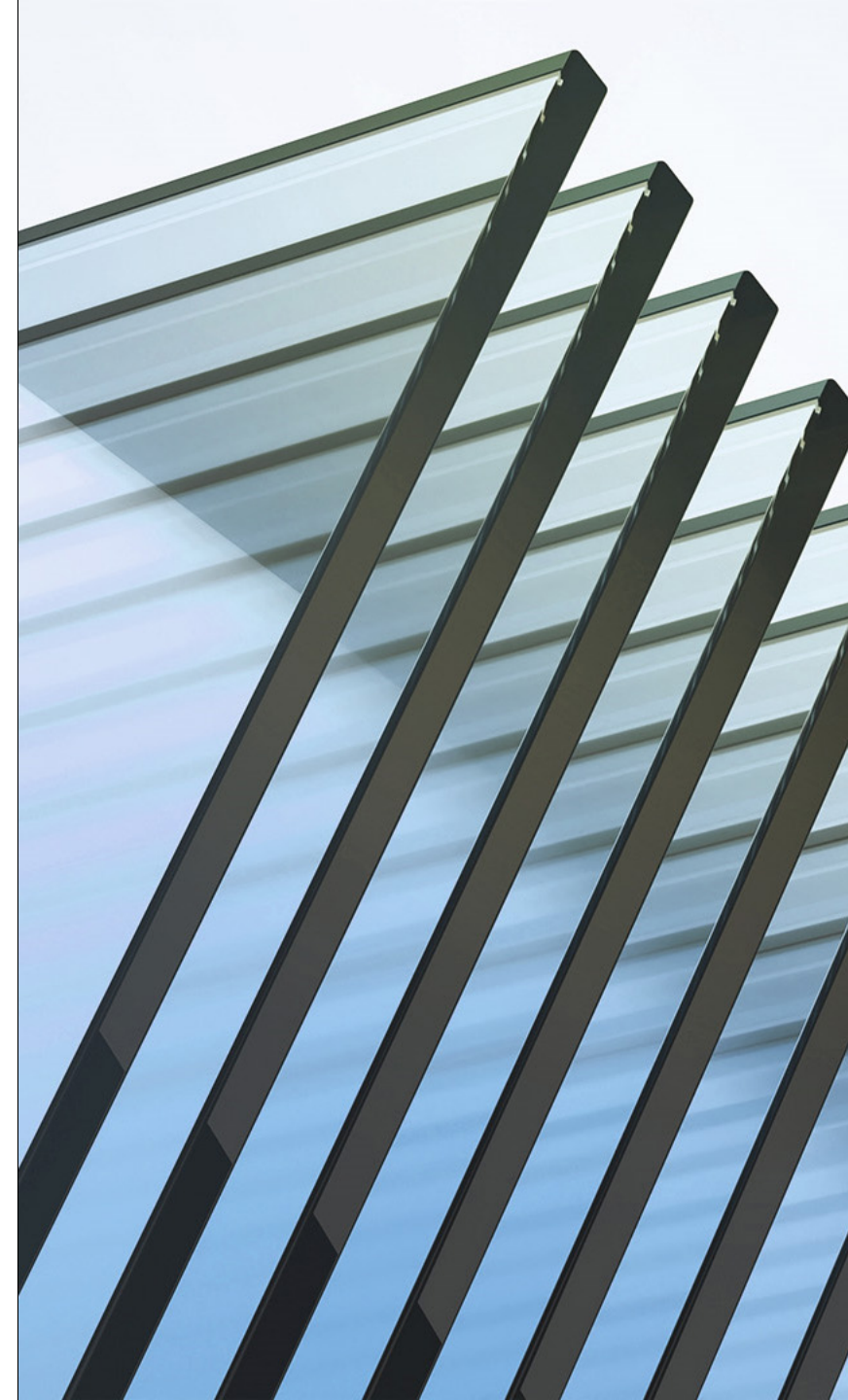
Broadening Horizons: Increased Insurance Access for Small Deals

- **Greater Appetite for Small Deals:** Insurers show an expanded interest in covering transactions below \$50M, diversifying the market base.
- **Lowered Barriers to Entry:** Initiatives to reduce minimum premium (\$100k or less in some transactions) and retention levels have made representation & warranty insurance more attainable for smaller transactions.
- **Adapted Coverage for Smaller Roll-Up Deals:** Certain insurance markets are attempting to introduce flexible policies catering to acquisitions below \$50M, aligning with sponsors' roll-up plans. Offers a master policy approach that seeks to significantly reduce the scope of the underwriting process for bolt-on transactions by allowing additional add-on transactions to be insured under a single policy.



Other Developments

- **Interim Breach:** In a transaction with a staggered sign-and-close, most policies historically included an exclusion for losses arising from an “Interim Breach”.
 - An Interim Breach requires that:
 - The facts and circumstances that caused the breach first occurred between signing and closing (the “interim period”); and
 - A member of buyer’s deal team obtained actual knowledge of the breach during the interim period
 - Certain markets now offer interim breach coverage (up to 30-45 days) for a fee (typically \$25k-\$50k of additional premium)
 - Additionally, certain excess policies can cover interim breach for up to 90 days
- **Deemed Modifications to Representations and Warranties:** Insurance markets are becoming increasingly focused on carving back representations that they perceive to be overly broad, leading to an increased focus on the changes proposed by each insurance market during the quotation phase.



GIBSON DUNN