GUNDERSON DETTMER

MAKING YOUR PRIVACY PROGRAM AI-READY

Practical Ways to Leverage Privacy Compliance for AI Regulations

November 12, 2025

Meet the Presenters

Cecilia Jeong
Data Privacy Attorney
cjeong@gunder.com

Frida Alim
Data Privacy Attorney
falim@gunder.com

Leila Golchehreh
Co-Founder & Chief Strategy Officer
leila@relyance.ail

GUNDERSON DETTMER

Clear Leader for the Innovation Economy

Gunderson Dettmer has decades of experience representing high-growth companies in their financings, IPOs and M&A transactions, and throughout their lives as public companies.

400
attorneys in
11 global markets

#1 GLOBALLY
most active law firm for venture capital financings every year since 2014 (PitchBook)

500+
venture capital and growth equity firm clients

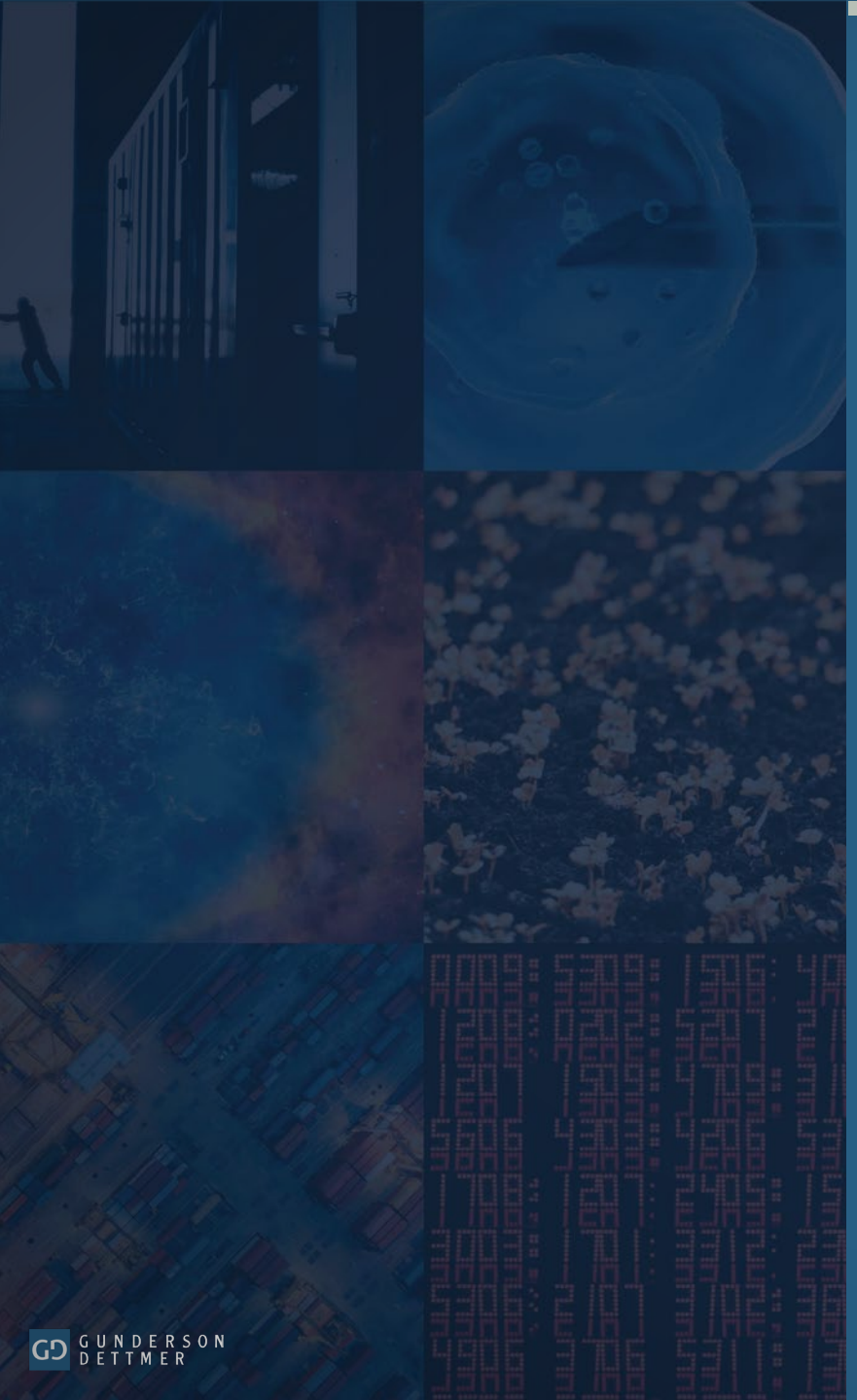
4,500+
company clients in the innovation economy worldwide

1,800+
venture financings for companies closed since 2022

$29B+
raised in venture financings for companies since 2022

300+
M&A transactions globally since 2022

GUNDERSON DETTMER



Agenda

1. Setting the Regulatory Stage

2. Assessing the Applicability of AI Laws

3. Leveraging Existing Infrastructure for AI Compliance

4. Additional Considerations under AI Laws

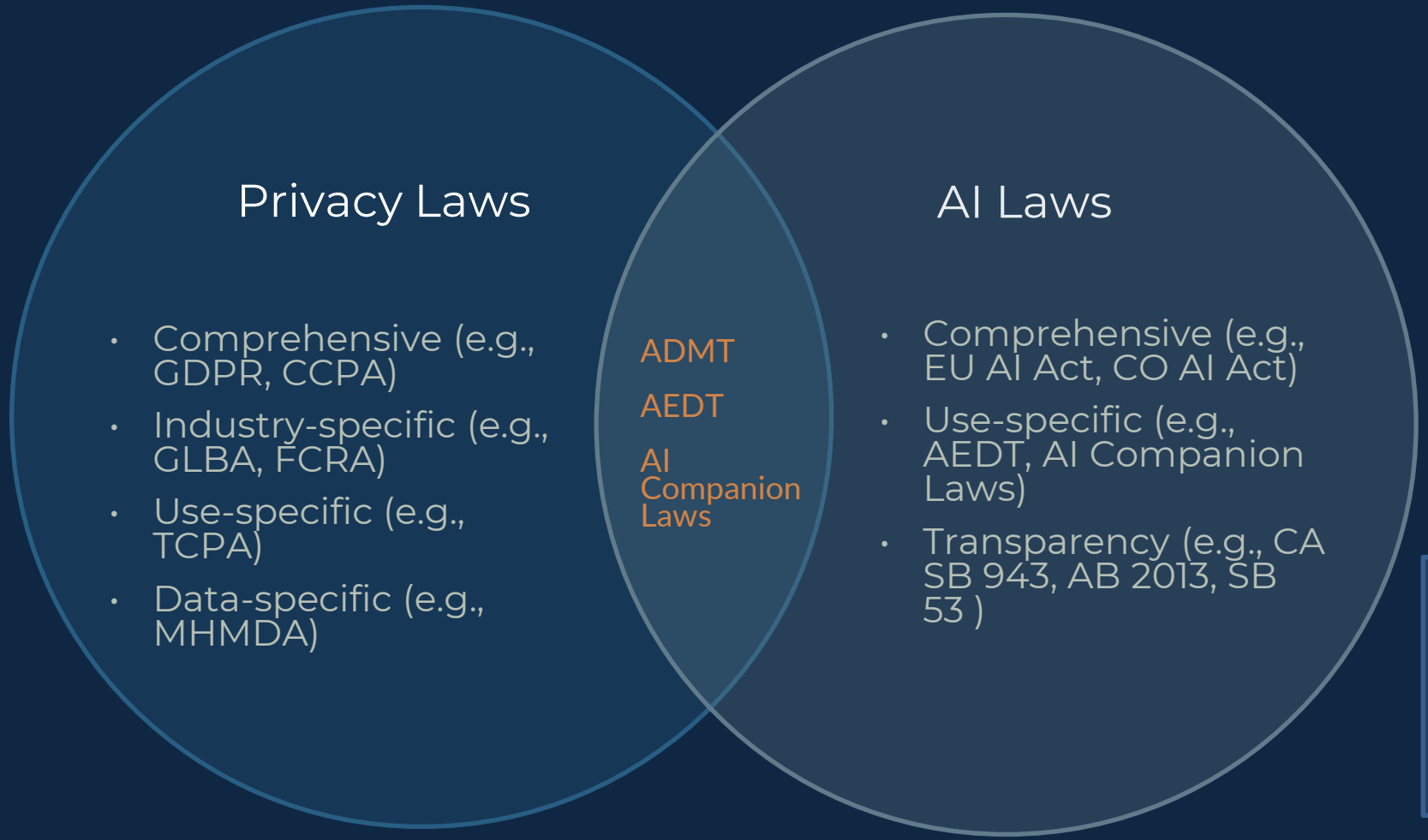
5. Top 5 Takeaways

6. Q&A

GUNDERSON DETTMER

Setting the Regulatory Stage

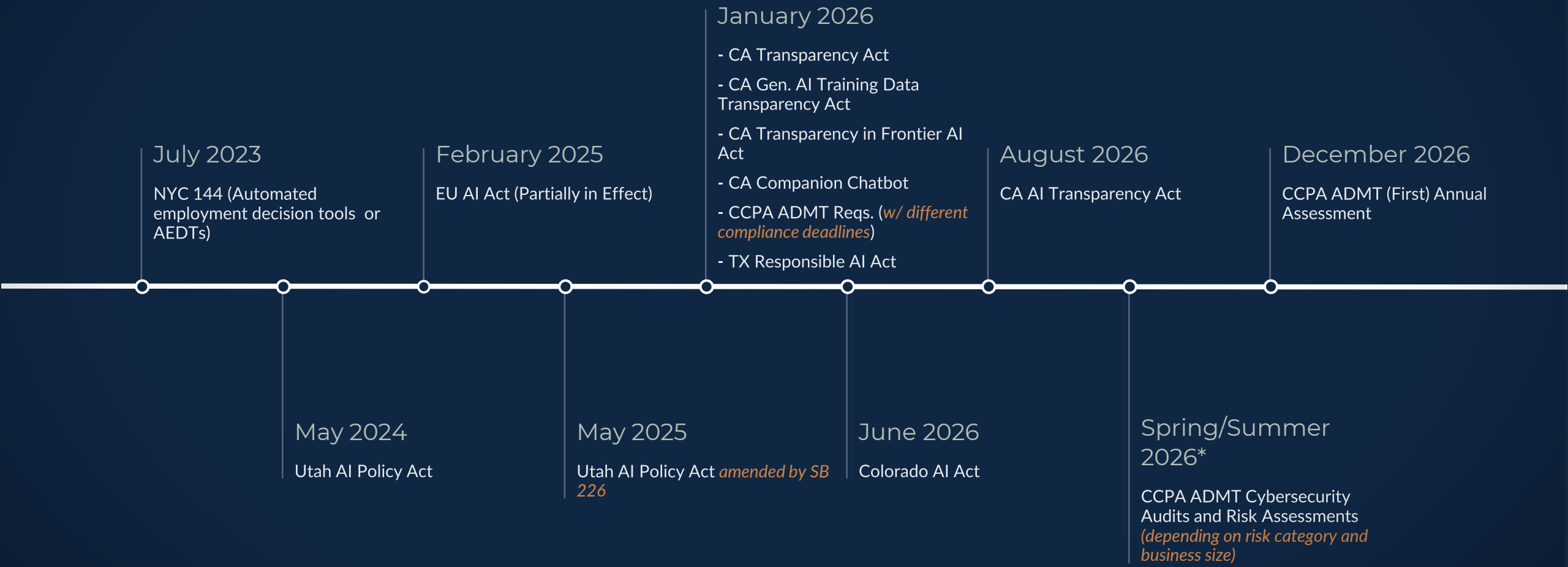
Intersection of Privacy and AI Laws

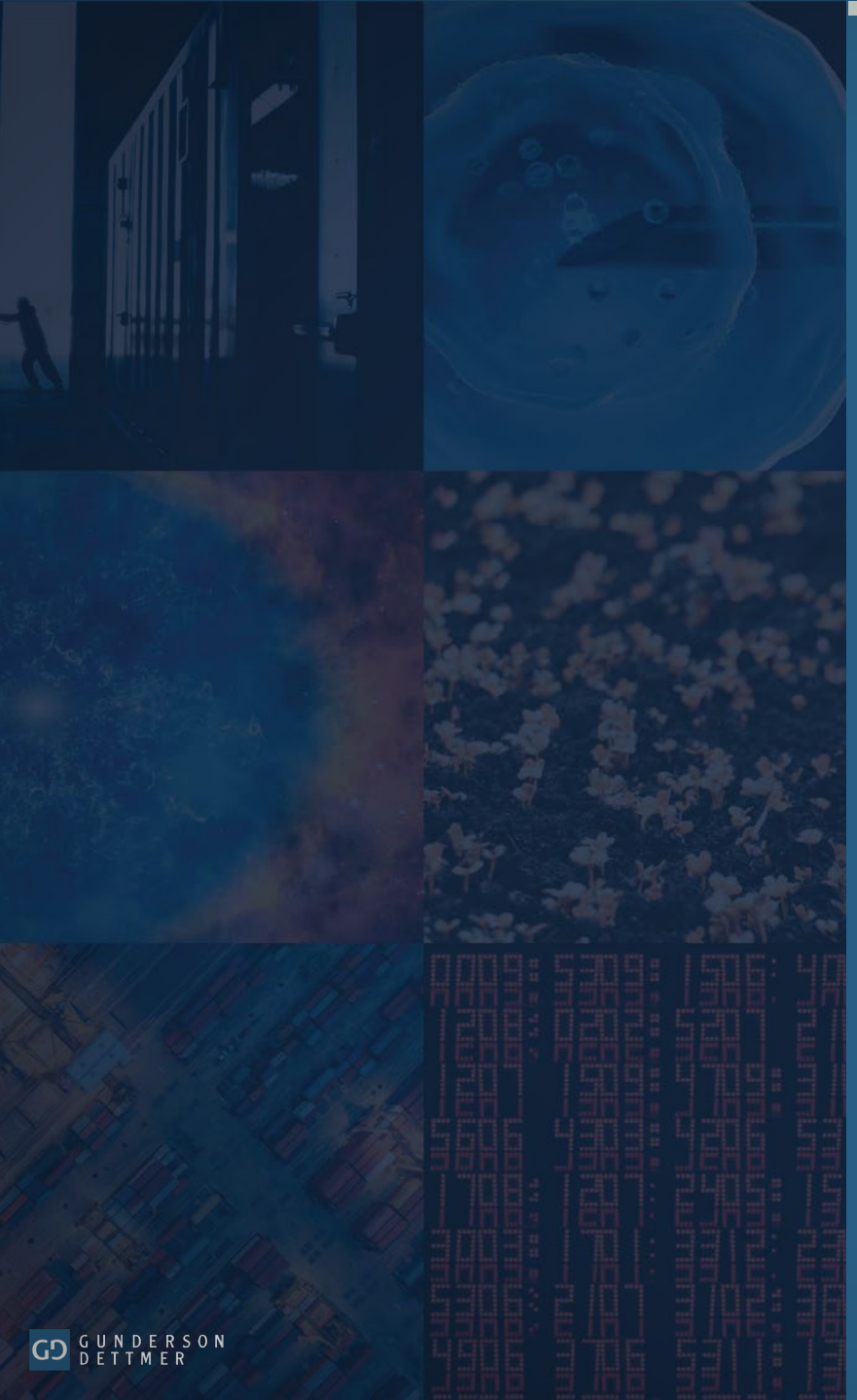


- ADMT = Automated Decision-Making Technology
- AEDT = Automated Decision-Making Tool

Setting the Regulatory Stage

Timeline of AI Laws





Agenda

1. Setting the Regulatory Stage
2. **Assessing the Applicability of AI Laws**
3. Leveraging Existing Infrastructure for AI Compliance
4. Additional Considerations under AI Laws
5. Top 5 Takeaways
6. Q&A

GUNDERSON DETTMER

How are companies approaching this mess?

1. Understand high risk areas
2. Assess applicability
3. Develop your AI posture
4. Consider common compliance areas

Understand High Risk Areas

Area	Core High-Risk Examples
Biometrics	Remote biometric identification (real-time or post-event, with limited exceptions). Biometric categorization based on sensitive or protected attributes (e.g., race, political opinion).
Critical Infrastructure	AI used as a safety component for the management and operation of road traffic, water, gas, heating, electricity, or critical digital infrastructure.
Education & Training	AI used for determining access to educational institutions or for evaluating learning outcomes (e.g., grading, exam proctoring).
Employment & HR	AI used for recruitment, candidate screening, evaluating performance, task allocation, or making decisions about promotion/termination.
Financial & Essential Services	AI used to evaluate creditworthiness (credit scoring, excluding fraud detection) or to evaluate eligibility for essential public assistance/benefits (e.g., healthcare, social services).
Law Enforcement	AI used for assessing the risk of an individual becoming a victim or re-offender, evaluating the reliability of evidence, or using polygraphs.
Migration, Asylum & Border Control	AI used to assess the security or irregular migration risk of a person or to assist in the examination of visa, asylum, or residence permit applications.
Justice & Democratic Processes	AI intended to assist judicial authorities in searching for, interpreting, or applying law and facts, or to influence the outcome of elections/referenda.

Assessing Applicability

Establish a Centralized AI Inventory + Map / Registry: Conduct an inventory of AI systems to eliminate "Shadow AI" and track their risk tier.

- Consider internal and external uses
- Don’t forget your vendors
- If feasible, work with a technology partner

Risk-Tiering – Both for Internal AI and External Third-Party Vendors, as well as Generative AI: Classify all in-house AI based on impact level (e.g., High-Risk, Customer decisions) to align mandatory oversight and review.

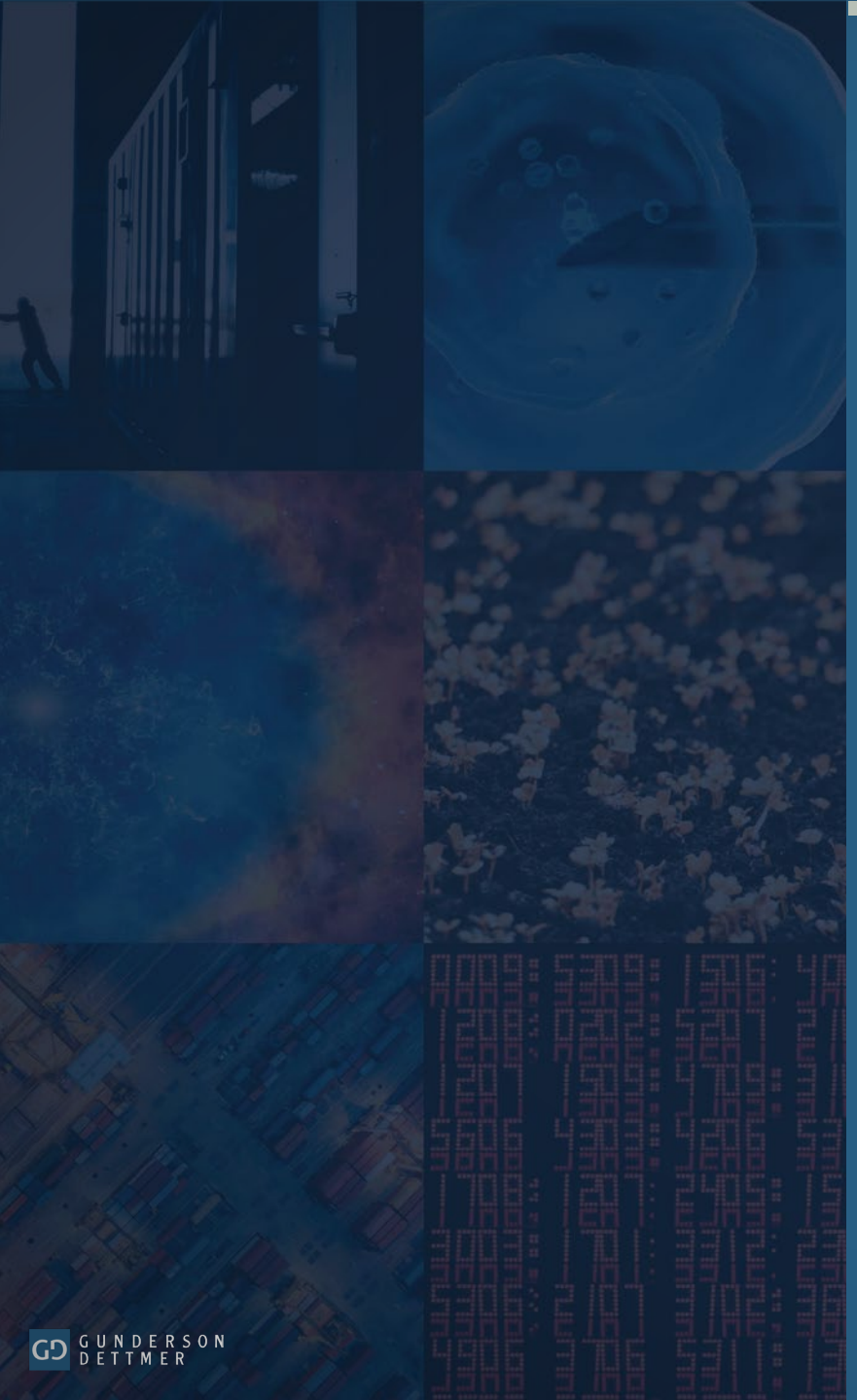
Third-Party Due Diligence: Integrate assessments into Vendor Risk Management (**VRM**) to audit how vendors use AI and what our data feeds into their systems.

Developing Your AI Posture

Developer	Deployer
• Develops or substantially modifies an AI system • Sells, licenses, or makes it otherwise commercially available for use	• Implements, puts the AI system into use, or uses AI system • Typically determines use (e.g., to make consequential decisions)

Common Compliance Areas

1. Transparency
2. Data subject rights (e.g., consents, opt-outs)
3. Risk assessments
4. Regular audits
5. Vendor management/flow down obligations



Agenda

1. Setting the Regulatory Stage
2. Assessing the Applicability of AI Laws
3. **Leveraging Existing Infrastructure for AI Compliance**
4. Additional Considerations under AI Laws
5. Top 5 Takeaways
6. Q&A

GUNDERSON DETTMER

Leveraging Existing Infrastructure for AI Compliance

Framework Component	Privacy Law Processes	AI Law Processes	Leveraging Privacy Processes for AI Compliance
Risk identification	• Data maps • PIAs • DPIAs • Legitimate interest assessments	• Impact assessments (e.g., COAIA) • Bias audits (e.g., NYC 144)	Leverage the following from privacy law processes: • Mapping of data flows • Cataloging of risks • Risk mitigation strategies
Transparency	• Notice at collection • Privacy policy • Just-in-time notices	For developers: • Disclosure of training data (sources, types) used to develop genAI models (CA Training Data Transparency Act). • On website, disclosure of (i) high-risk systems developed or made available, (ii) risk management for discrimination (COAIA). For deployers: • Disclosure that consumer is interacting with AI system (various laws). • For high-risk AI systems, notification to consumer before a consequential decision is made (e.g., COAIA, CCPA). *Note that some laws require specific documentation be made available to regulatory bodies (e.g., COAIA, EU AI Act).*	• Ensure AI notices align with existing privacy notices • Supplement privacy notices with AI disclosures (e.g., appeals process, data subject rights, where to submit AI related inquiries) • Consider appropriate placement/timing for presenting AI-related notices

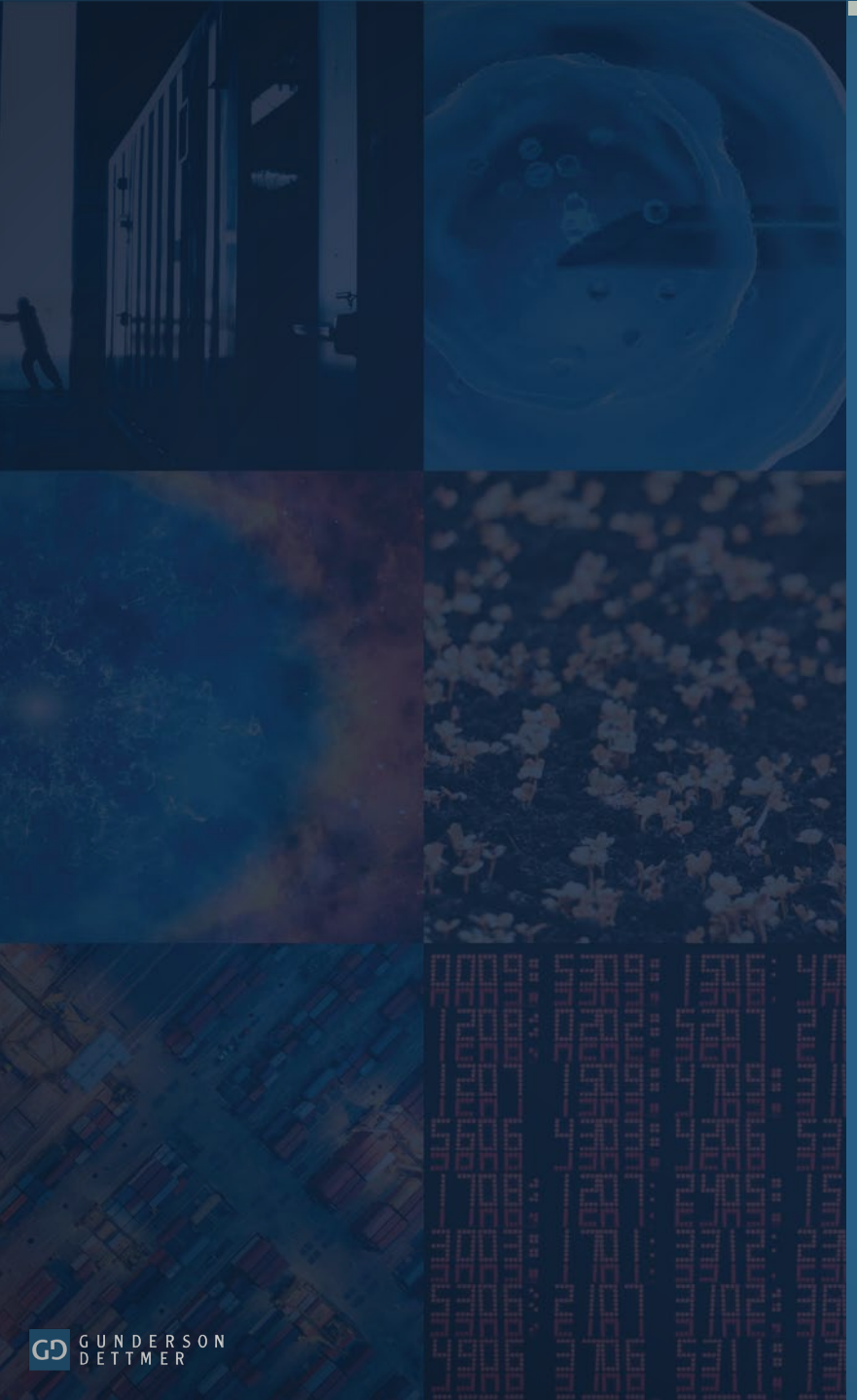
Leveraging Existing Infrastructure for AI Compliance

Framework Component	Privacy Law Processes	AI Law Processes	Leveraging Privacy Processes for AI Compliance
Vendor Management	Processor flow-down terms, e.g.: • Data use restrictions • Data retention • Sub-processor notifications • auditing/oversight	Same + restrictions on: • Data use and training • Retention (e.g., ZDR)	Leverage and supplement existing vendor questionnaires with Qs on: • Whether vendor is a provider or deployer • Whether AI is “high-risk” • Training data sources (will data we provide be used?) • The vendor’s data governance framework
Data subject rights	• Right to access • Right to correct • Right to delete • Right to opt-out of selling/sharing • Right to appeal	• Right to correct data • Right to appeal adverse consequential decision (+ human review) • Right to opt-out of automated profiling by high-risk AI systems	Reuse privacy DSR workflows to handle access/opt-out rights and appeal pathways while noting deviations in: • Timelines for responding • When/where to offer DSR mechanisms
Stakeholder Engagement	Consult with: • Engineering (data scientists, cyber) • Marketing/Sales (e.g., prospecting tools, recording tools) • Executive leadership/board • Legal • Security • Human resources • Procurement	Similar.	Same group, new questions, e.g.: • Where is this model sold? • What is the purpose of the model? • How is the model being used and intended to be used? • How was the AI model trained and validated? What are the outputs? • What are the model’s limitations and risks? • Is it obvious to users that they are dealing with AI?

Leveraging Existing Infrastructure for AI Compliance

Bridging PIAs and AI Risk Assessments

Traditional PIA Components:	AI Risk Assessments:
• Map data flows • Describe the processing: the how and why • Describe the context and purpose of the processing • Identify the source of risk and nature of potential impact on individuals • Necessity and proportionality of processing • Risk mitigation (safeguards, security measures)	• Map data flows (including training data, inputs and outputs) • Describe the processing (purpose, intended use cases, benefits) • Identify metrics and known limitations • Identify known or reasonably foreseeable risks of algorithmic discrimination • Risk mitigation • Transparency mechanisms for explainable AI • Post-deployment monitoring and user safeguards, including oversight, use and learning processes to address issues from deployment. **Timing (for CO AI Act)**: Before deploying or substantially modifying a high-risk AI system, then, at least annually and within 90 days after any substantial modification.



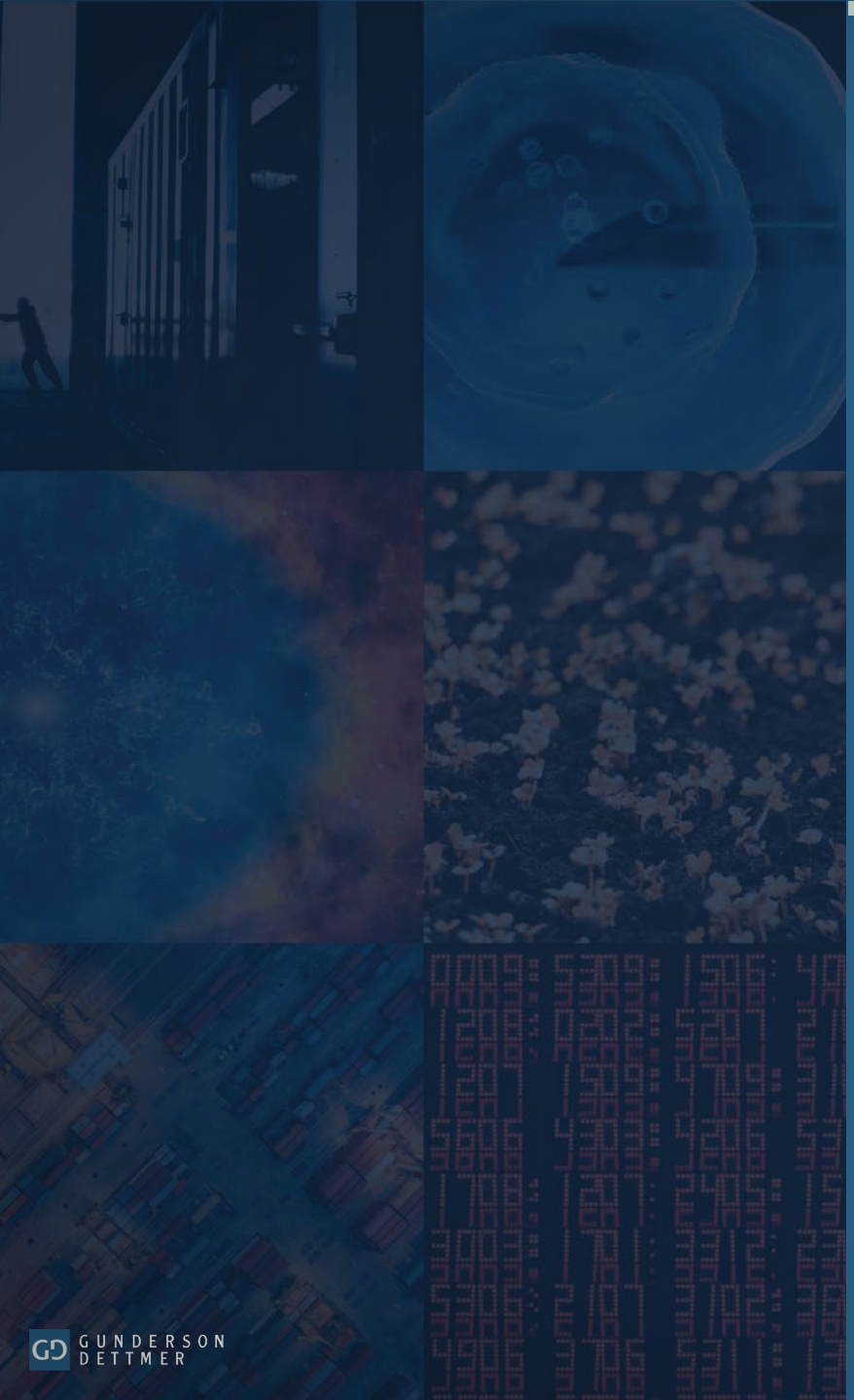
Agenda

1. Setting the Regulatory Stage
2. Assessing the Applicability of AI Laws
3. Leveraging Existing Infrastructure for AI Compliance
4. **Additional Considerations under AI Laws**
5. Top 5 Takeaways
6. Q&A

GUNDERSON DETTMER

Additional Considerations under AI Laws

- Explainability
- Bias & Non-Discrimination
- Safety & Risk Management
- Accuracy & Hallucinations
- Accountability, Reliability & Control
- Transparency of Content
- Ethics & Data Governance



Agenda

1. Setting the Regulatory Stage
2. Assessing the Applicability of AI Laws
3. Leveraging Existing Infrastructure for AI Compliance
4. Additional Considerations under AI Laws
5. **Top 5 Takeaways**
6. Q&A

GUNDERSON DETTMER

Top 5 Takeaways

1. **Knowledge is power**
    - Understand how AI is leveraged by your business
    - Understand data use
2. **Teamwork makes the dreamwork**
    - Work with your stakeholders
    - Engage legal - internal and external
    - Identify the tools available to you that can help
3. **Simplify to amplify**
    - Develop your posture
    - Identify your principles
4. **Clarity through priorities**
    - Implement compliance measures by priority
5. **Stay nimble**
    - Monitor and adjust as needed
    - Compliance is a moving target as law and technology change

List of AI Resources

A. AI Courses

a. AI Academy (IBM)
b. Google AI Essentials
c. Coursera

B. Foundational Ethics & Frameworks

- ABA Law and AI Resources:
  - Essential guidance on professional responsibility and ethical duties for lawyers using Generative AI.
  - Link: ABA Law and AI Resources
- NIST AI Risk Management Framework (AI RMF):
  - The leading, non-sector-specific framework for establishing internal AI governance and compliance programs (referenced by the EU AI Act).
  - **Link: NIST AI RMF 1.0 (via ABA)**

C. Key Certifications (Industry Standards)

- IAPP: AI Governance Professional (AIGP):
  - The premier certification demonstrating expertise in legal, ethical, and operational management of AI systems.
  - Link: AIGP Certification - IAPP
- Georgetown SCS: AI Governance & Compliance Certificate:
  - A comprehensive program for lawyers and compliance professionals covering global legal/ethical requirements.
  - Link: Georgetown Certificate in AI Governance

D. Regulatory Tracking & Analysis

- Thomson Reuters Legal Insights:
  - Provides continuous expert analysis on risk mitigation, legal tech, and the intersection of AI with the legal profession.
  - Link: Thomson Reuters Legal AI Tools

Questions?