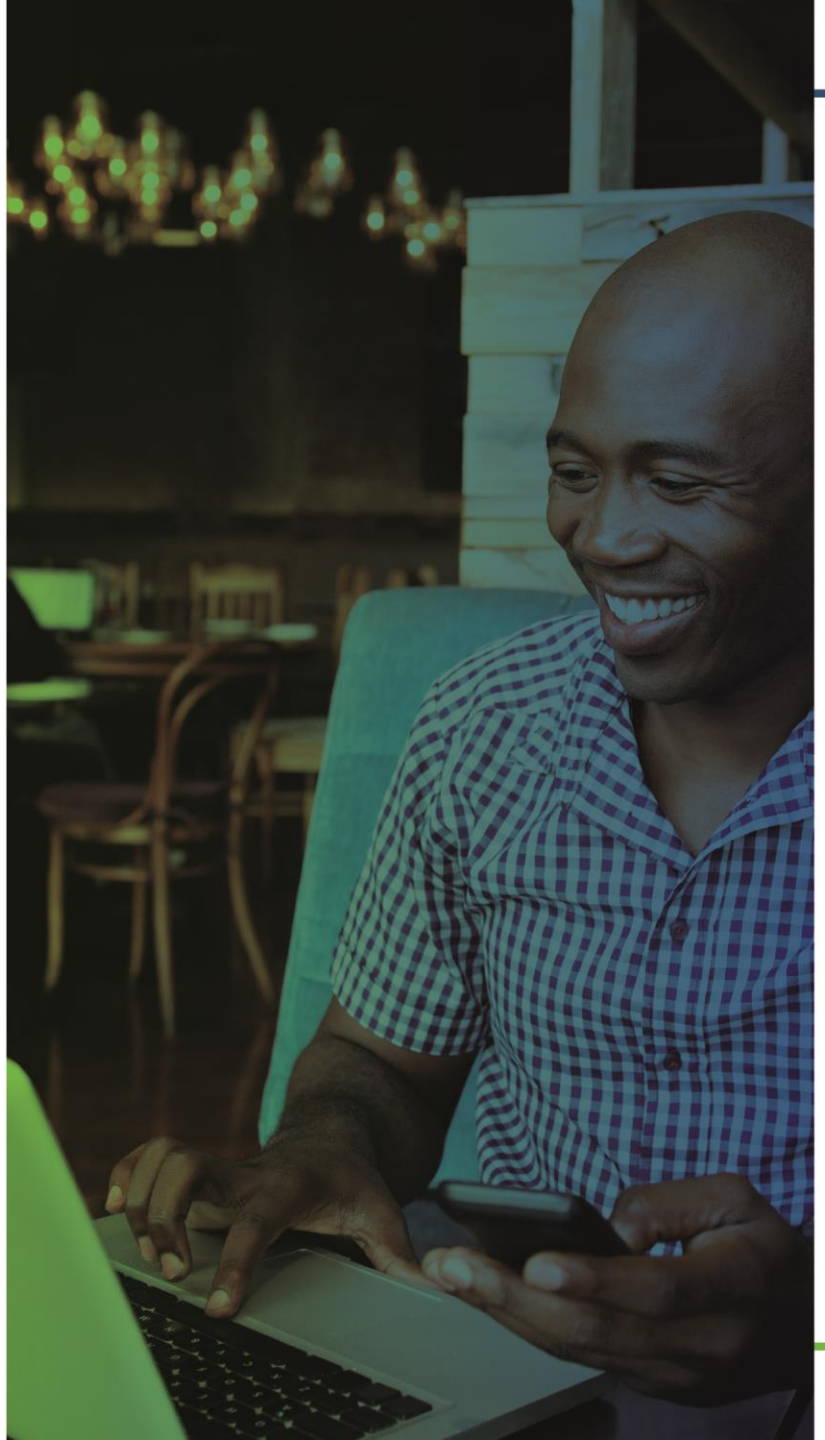
osano



Midyear Data Privacy Check-in: Trends And Key Updates

Thursday, 13 June
10:00–11:00 PST
13:00-14:00 EST
19:00–20:00 CET

Presented by

Rachael Ormiston

Head of Privacy

Osano

CIPP/E, CIPP/US, CIPM, FIP

Joshua Vaughan

Senior Data Privacy Consultant

Zaviant

CIPP/US, JD

osano

Agenda

- The Basics of Data Privacy in 2024
- What to Prepare for Now
- Enforcement
- What to Keep an Eye on
- Q&A

osano

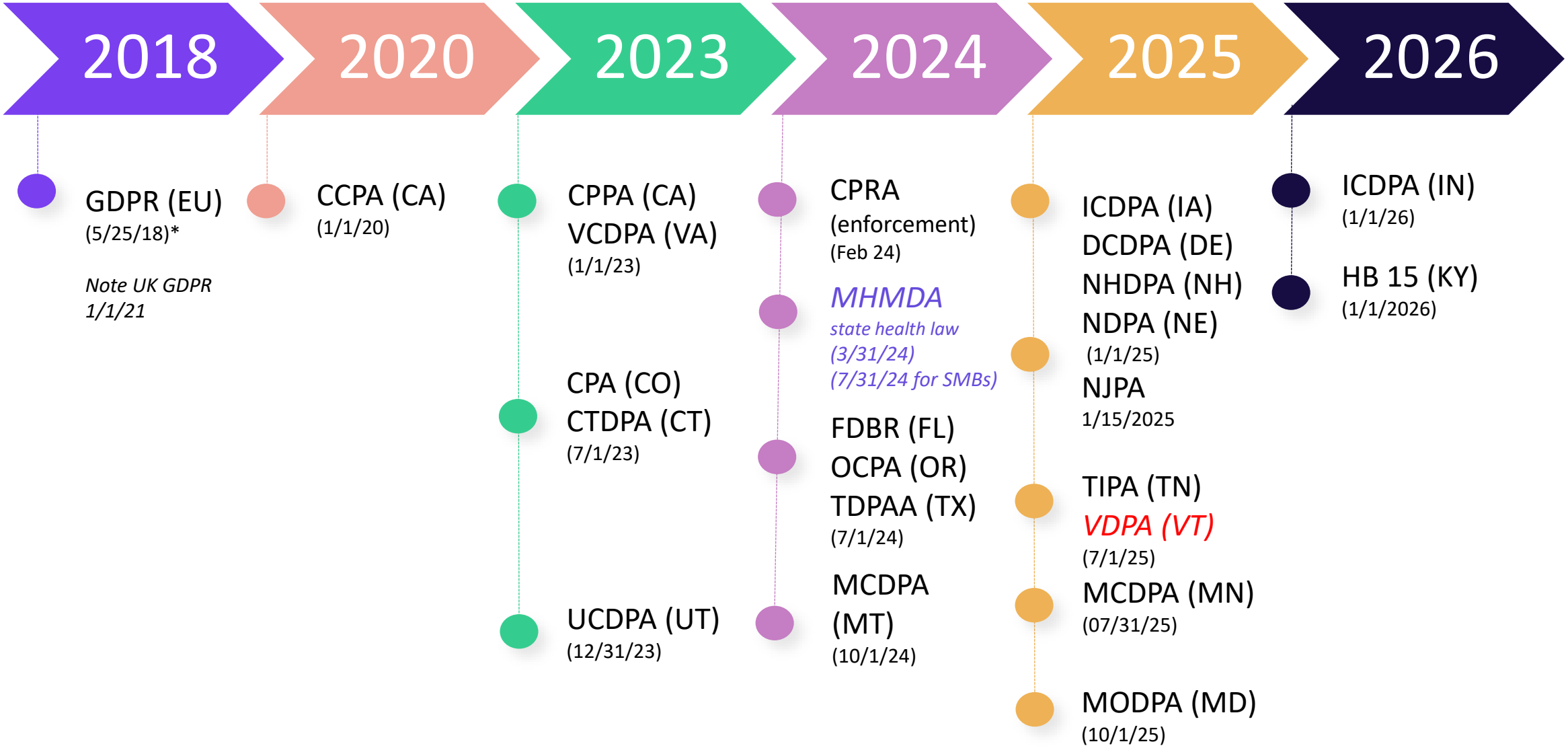
Poll

How Prepared Do You Feel For the Second Half of the Year?

1. I'm ready for anything
2. Very prepared
3. Somewhat prepared
4. Not very prepared
5. Totally out of the loop

osano

20 consumer US state comprehensive privacy laws



osano

Key Components of a Data Privacy Law

Definitions

1. Which organizations are subject to the law, and which are exempt?

2. Who is protected by the law?

3. What constitutes personal information?

4. What constitutes sensitive information?

Requirements

5. What kind of consent do you need?

6. What rights do consumers have?

7. How are data transfers handled?

Enforcement

8. What are the penalties associated with breaking the law?

9. Who enforces the law?

What To Prepare For Now

Laws Going Into Effect H2 2024

H2 2024 State Privacy Laws at a Glance

Feature	Texas (TDPSA)	Oregon (OCPA)	Montana (MTCDPA)
Thresholds	Conduct business in Texas or produce products/ services consumed by residents, OR process or engage in the sale of personal data AND are not small businesses. ***No Revenue Thresholds***	• Control/process the personal data of 100,000 or more residents, OR • 25,000 or more residents, while deriving 25% or more of gross revenue from selling personal data.	• Control/process the personal data of at least 50,000 residents, OR • 25,000 or more residents and derive more than 25% of gross revenue from selling of personal data.
Fines	Up to $7,500 per violation + injunctive relief to restrain or enjoin the violator's operations	Up to $7,500 per violation	Not yet specified
Cure Period	30 days, **no sunset**	30 days, sunsets Jan. 2026	60 days, sunsets April 2026
Data Processing Agreements	Yes	Yes	Yes

osano

H2 2024 State Privacy Laws at a Glance

Feature	TDPSA	OCPA	MTCDPA
Data Protection Assessments	Required for targeted advertising, sale of data, profiling, sensitive data processing, other processing activities with risk of harm to consumers.	Required for targeted advertising, sale of data, profiling, sensitive data processing, other processing activities with risk of harm to consumers.	Required for targeted advertising, sale of data, profiling, sensitive data processing, other processing activities with risk of harm to consumers.
Recognize Universal Opt-Out Mechanisms	Yes, as of January 1, 2025	Yes, as of January 1, 2026	Yes, as of January 1, 2025
Sensitive Data	• Racial or ethnic origin • Religious beliefs • Mental/physical health condition and medical treatment, diagnosis by HCP • Sexuality • Citizenship/immigration status • Genetic or biometric data • Personal data of a known child • Precise geolocation	• Racial, ethnic, national origin • Religious beliefs • Mental/physical health condition, diagnosis, medical history and/or treatment, diagnosis by HCP • Sexual orientation and status as transgender/nonbinary • Citizenship/immigration status • Genetic or biometric data • Personal data of a known child • Precise geolocation • Status as victim of a crime	• Racial or ethnic origin • Religious beliefs • Mental/physical health condition and/or diagnosis • Sexual orientation, sex life, sexuality • Citizenship/immigration status • Genetic or biometric data • Personal data of a known child • Precise geolocation

H2 2024 State Privacy Laws at a Glance

Feature	TDPSA	OCPA	MTCDPA
Know/Access	✓	✓	✓
Delete	✓	✓	✓
Correct	✓	✓	✓
Opt Out of Sale	✓	✓	✓
Opt Out of Targeted Advertising	✓	✓	✓
Opt Out of Profiling	✓	✓	✓

H2 2024 State Privacy Laws at a Glance

Feature	TDPSA	OCPA	MTCDPA
Obtain a list of third parties that received personal data	✗	✓	✗
Opt into sensitive data processing	✓	✓	✓
Right to object to automated decision-making/profiling	✓	✓	✓
Response Time	45 days, extendable by another 45 days if high volume/complexity is demonstrated.	45 days, extendable by another 45 days if high volume/complexity is demonstrated.	45 days, extendable by another 45 days if high volume/complexity is demonstrated.

Practical Advice for Compliance

1. Map Your Data

- Conduct a data inventory
- Where do you collect, process, store, and transfer data?

2. Review Your Privacy Policy

- Does it accurately reflect your processing activities?
- Purpose and legal basis?
- Data retention policies?

3. Manage Consent

- Do you collect personal information via cookies? What about other channels?
- Can you recognize and act on universal opt-out mechanisms?

4. Prepare for PIAs

- Required for processing that presents a "heightened risk of harm" to the consumer
- Identify data processing activities in your data map that require PIAs.
- Conduct trial PIAs.

5. Assess Your DSAR Workflow

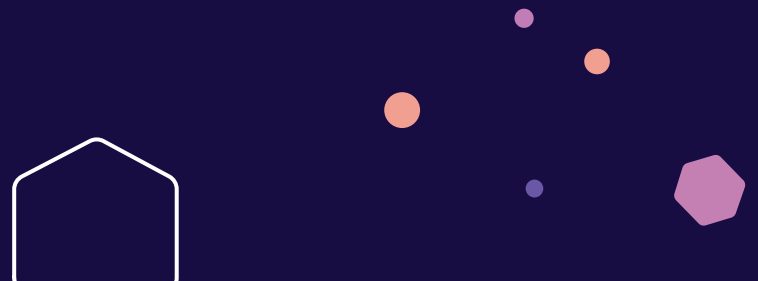
- Can you process requests within 45 days?
- Will you acknowledge DSARs from non-covered jurisdictions, or will you take the time to triage?
- Conduct a trial DSAR to find out where your gaps lie.

6. Build Awareness

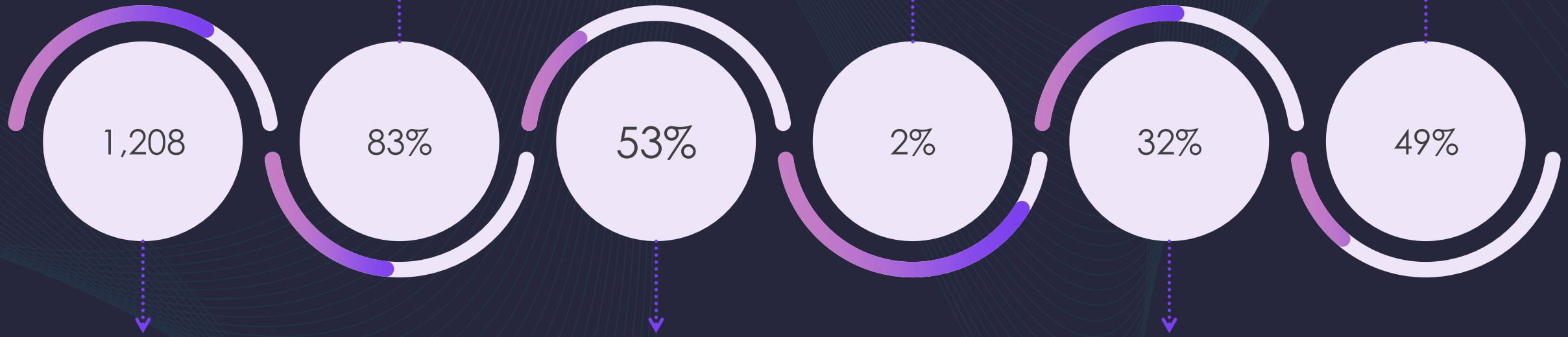
- Provide scalable training for PIAs, data mapping, consent governance, etc.
- Secure the business buy-in for investment as privacy obligations continue to evolve

Enforcement

How to Prepare and What to Expect



CPPA Enforcement Report



Complaints

July 6, 2023–February 22, 2024

17% Non-CA residents

California Residents

Right to Delete

Most common, followed by selling/sharing of personal information

Least common, followed by right to correct

Financial Incentive/loyalty program

Familiarity with CPPA

47% unfamiliar and 21% indifference

20-31% have requested deletions or other rights

Exercised DSNMI

Enforcement Update & Priorities. 2024, CPPA.

Sephora vs. Doordash

	Sephora (August 2022)	Doordash (February 2024)
	CPPA	CPPA + CalOPPA
Violations	Had third party trackers on its site with no do-not-sell (DNS) link, no GPC.	Shared data with two marketing co-ops to benefit from targeted ads to consumers of the other marketing co-op participants
Takeaways	GPC—right to opt out of the sale of their personal information is the "hallmark of the CCPA	Exchange for value (incl. benefit of advertising)= sale
Cured?	No	No
Fine	**$1.2m** **+ remedial measures** *online disclosure and opt-out practices*	**$375K** **+ injunctive remedies** *(comply with regs, review contracts with marketing and analytics vendors, use technology when selling/sharing consumer personal information, annual reports to AG.*

osano

What Can We Expect From Other Regulators?

FTC Enforcement

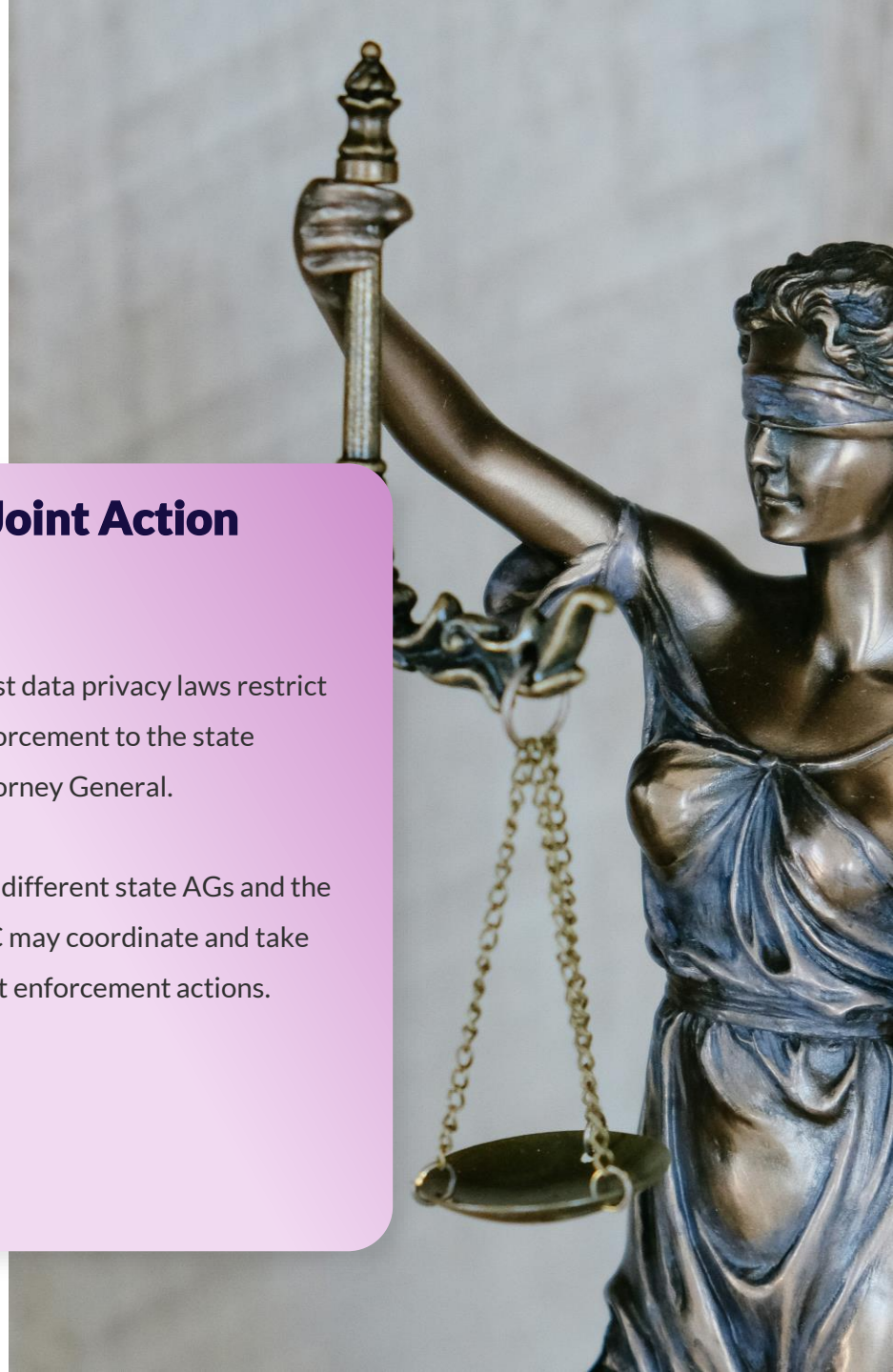
- January: X-Mode Social, Inc./Outlogic settles with FTC over sale of sensitive personal information
- February: Avast Limited banned from selling browsing data, ordered to pay $16.5 million
- May: FTC fires 'shot across the bow' at automakers over connected-car data privacy Blackbaud, Inc. ordered to adhere to data minimization, transparency principles post-breach

Texas Task Force

"Any entity abusing or exploiting Texans' sensitive data **will be met with the full force of the law.** Companies that collect and sell data in an unauthorized manner, harm consumers financially, or use artificial intelligence irresponsibly present risks to our citizens that we take very seriously."
- Texas Attorney General Ken Paxton

Joint Action

- Most data privacy laws restrict enforcement to the state Attorney General.
- But different state AGs and the FTC may coordinate and take joint enforcement actions.



What to Keep an Eye on

Major Developing & Proposed Laws

Upcoming Data Privacy Laws

= Signed into law in 2024

Jan. 2025 ... Jul. 2025 ... Oct. 2025 ... Jan. 2026

Jan. 1

- Nebraska Data Privacy Act (NDPA)
- New Hampshire Privacy Act (NHPA)
- Iowa Consumer Data Protection Act (ICDPA)
- Delaware Personal Data Privacy Act (DPDPA)

Jan. 15

- New Jersey Data Protection Act (NJDPA)

Jan. 31

- Minnesota Consumer Data Privacy Act (MCDPA)

Jul. 1

- Tennessee Information Protection Act (TIPA)

Oct. 10

- Maryland Online Data Privacy Act (MODPA)

Jan. 1

- Kentucky Consumer Data Protection Act (KCDPA)
- Indiana Consumer Data Protection Act (ICDPA)

The American Privacy Rights Act

Bipartisan & Bicameral, But Far From Finished

- Applies to all businesses subject to the FTC, excluding small businesses
- Excludes:
  - Deidentified, publicly available, employee information
    - Would allow for state preemption (i.e., CPRA)
  - Inferences made from multiple independent sources
  - Information in a collection (e.g., library, museums, archives)
- Robust data minimization principles

Special Requirements for Large Data Holders

- LDHs:
  - Have $250 million or more in annual revenue;
  - Collect, process, retain, or transfer the covered data of millions individuals/devices or collect, process, retain, or transfer the sensitive data of hundreds of thousands of individuals/devices.
- Added requirements around reporting, PIAs, privacy policies, and more.

EU AI Act

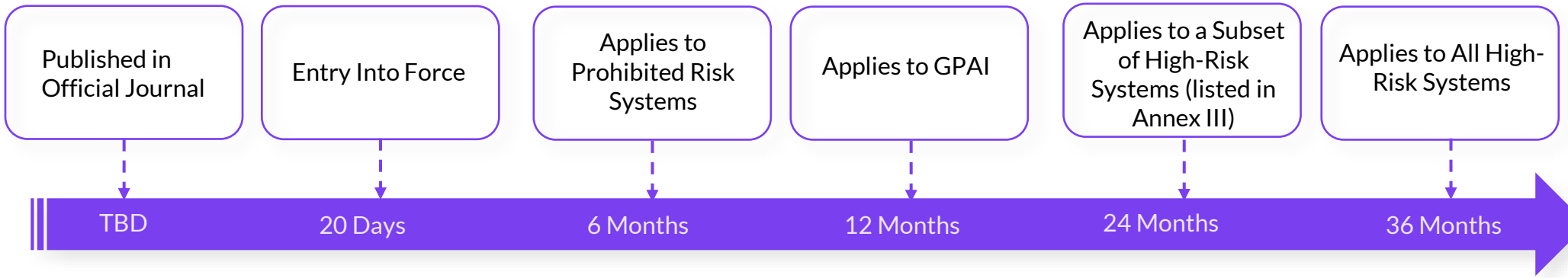
Major Features

- 4 Risk Levels: Unacceptable, High-Risk, Limited Risk, Minimal Risk
- Providers/developers of high-risk systems face the most obligations.

  Applies to:
  - Providers/developers who put high-risk systems into service in the EU
  - Providers/developers of high-risk systems whose output is used in the EU
  - Like GDPR, the law is extraterritorial
- Users (i.e., deployers of systems; not end-users) also face some obligations

Special Requirements for General Purpose AI (GPA)

- Special requirements for General Purpose AI (GPAI). Providers must:
  - Provide technical documentation on training, testing, etc.
  - Provide documentation to downstream providers to enable compliance.
  - Establish a policy to respect the Copyright Directive.
  - Publish a summary of training content.
- GPAI with significant training data may be classified as presenting "systemic risks"
  - Additional testing, risk mitigation, incident reporting, and cybersecurity.

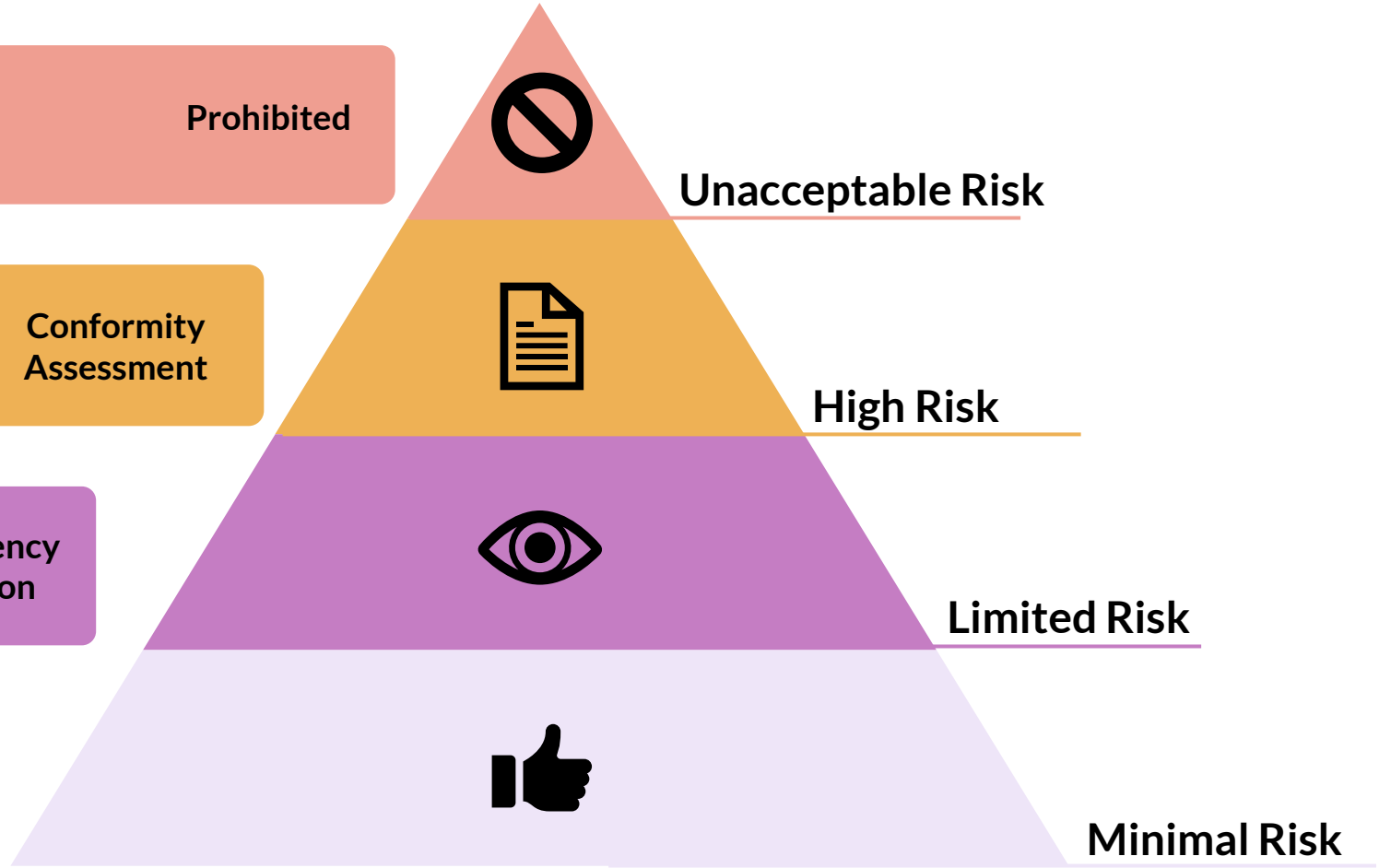


osano

Risk Assessments

EU AI Act Risk Levels

Social scoring, mass surveillance, manipulation of behavior causing harm	**Prohibited**
Access to employment, education and public services, safety components of vehicles, law enforcement, etc.	**Conformity Assessment**
Impersonation, chatbots, emotion recognition, deep fakes	**Transparency Obligation**
Remaining	**No Obligation**



osano

CO AI Act

Key Definitions

- "Algorithmic Discrimination"
- "Consequential Decision"
- "High-Risk Artificial Intelligence System"

Developer Obligations

- Have a "duty of care"
- Disclosures to developers
  - Contracts, statements, PIA enablement
- Public disclosures
  - General statement on appropriate/inappropriate uses of high-risk AIs
  - Documentation describing characteristics of training data, intention, limitations
  - Assessments of high-risk AIs (e.g., intended outputs, risk mitigation, algorithmic discrimination)
- Notifications of algorithmic discrimination

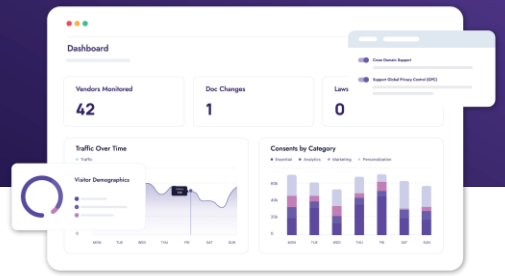
Enforcement

- Goes into effect February 1, 2026
- AG Enforcement
  - Civil penalty up to $20K per violation

Deployer Obligations

- Have a "duty of care"
- Establish a risk management program for high-risk AIs
- Conduct impact assessments
  - Annually and within 90 days of modification of AIs
- Disclosures—public and directly to consumer
- Consumer rights
  - Right to opt out of high-risk AI consequential decision-making
  - Upon adverse consequential decisions: Notice/description; Opportunity to correct incorrect data involved; Opportunity to appeal decision.
- Notifications of algorithmic discrimination to attorney general

Stay In Touch and Learn More!



[Schedule a Demo](#)

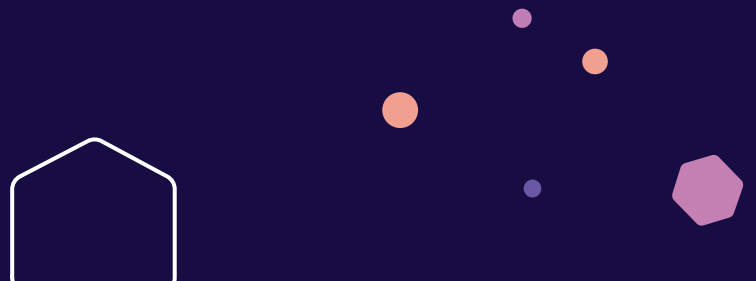
Contact Zaviant

[Check out the Osano Blog](#)

osano

Q&A

Ask your most pressing data privacy questions.



Web Conference
Participant Feedback Survey

Please take this quick (2 minute) survey to let us know how satisfied you were with this program and to provide us with suggestions for future improvement.

Click here: https://iapp.questionpro.com/t/AOhP6Z2njp

Thank you in advance!

For more information: www.iapp.org

Attention IAPP Certified Privacy Professionals:

This IAPP web conference may be applied toward the continuing privacy education (CPE) requirements of your CIPP/US, CIPP/E, CIPP/A, CIPP/C, CIPT or CIPM credential worth 1.0 credit hour. IAPP-certified professionals who are the named participant of the registration will automatically receive credit. If another certified professional has participated in the program but is not the named participant then the individual may submit for credit by submitting the continuing education application form here: submit for CPE credits.

Continuing Legal Education Credits:

The IAPP provides certificates of attendance to web conference attendees. Certificates must be self-submitted to the appropriate jurisdiction for continuing education credits. Please consult your specific governing body's rules and regulations to confirm if a web conference is an eligible format for attaining credits. Each IAPP web conference offers either 60 or 90 minutes of programming.

For questions on this or other
IAPP Web Conferences or recordings
or to obtain a copy of the slide presentation
please contact: livewebconteam@iapp.org

Thank You!

osano