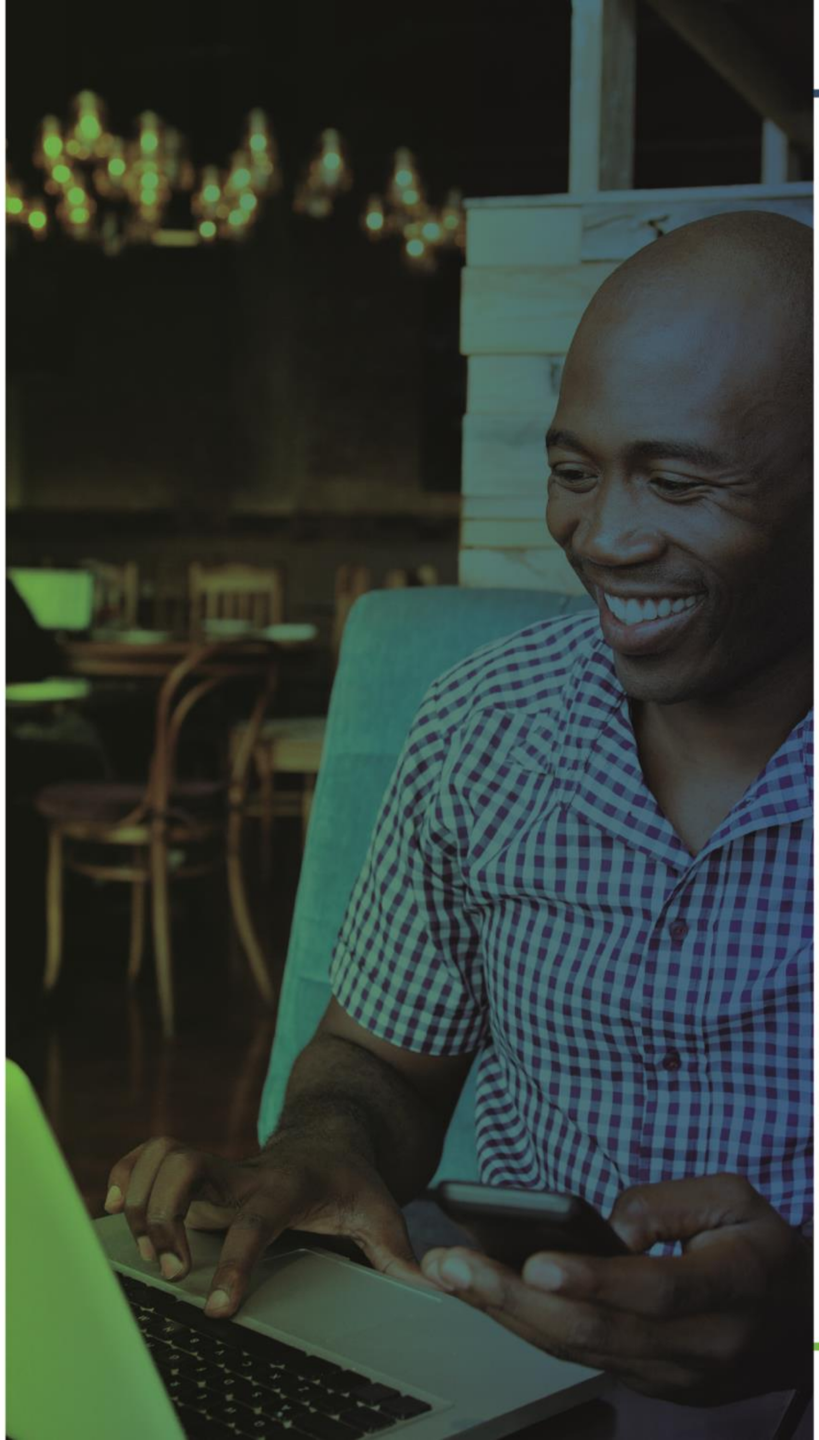
osano



iapp

The Cost of Noncompliance: More Than Just Fines

Thursday, 27 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

Amy de La Lama

Partner: Chair—Global Data Privacy & Security

BCLP.

Daniel Rockey

Partner: Litigation, Regulatory & Privacy

BCLP.

Agenda

- The Changing Legal Landscape
- Fines: How They're Determined and Handed Out
- Why Noncompliance Goes Beyond Fines
- Enforcement Actions and Litigation
- Practical Tips for Achieving Compliance
- Q&A

Poll

What’s the Biggest Driver Behind Your Organization’s Data Privacy Program?

1 Business ethics

2 Competitive advantage

3 Avoiding fines

4 Avoiding negative press and protecting our brand

5 Other

There Are Lots of Reasons to Become Compliant…

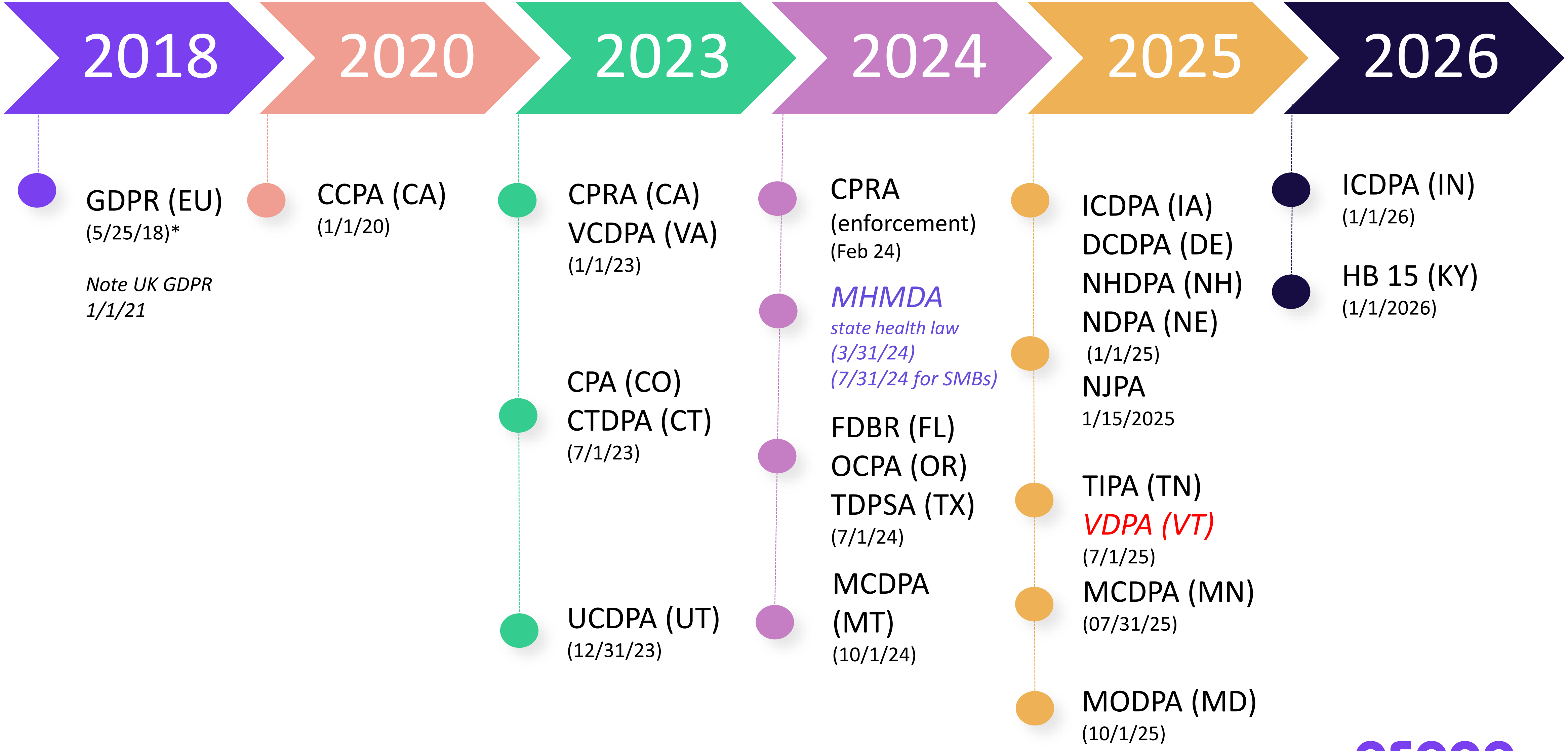
- Improving customer trust
- Conducting your business in an ethical way
- Stronger position in business deals
- Tangential benefits like stronger data governance

… But Avoiding Financial Penalties Is Often the Most Persuasive

- Especially for non-privacy experts in the business
- That's why we're focusing on costs in this webinar

2024 | The Cost of Noncompliance: More Than Just Fines

The Changing Legal Landscape



2018

GDPR (EU)
(5/25/18)*

*Note UK GDPR
1/1/21*

2020

CCPA (CA)
(1/1/20)

2023

CPRA (CA)
VCDPA (VA)
(1/1/23)

CPA (CO)
CTDPA (CT)
(7/1/23)

UCDPA (UT)
(12/31/23)

2024

CPRA
(enforcement)
(Feb 24)

*MHMDA
state health law
(3/31/24)
(7/31/24 for SMBs)*

FDBR (FL)
OCPA (OR)
TDPSA (TX)
(7/1/24)

MCDPA
(MT)
(10/1/24)

2025

ICDPA (IA)
DCDPA (DE)
NHDPA (NH)
NDPA (NE)
(1/1/25)
NJPA
1/15/2025

TIPA (TN)
VDPA (VT)
(7/1/25)

MCDPA (MN)
(07/31/25)

MODPA (MD)
(10/1/25)

2026

ICDPA (IN)
(1/1/26)

HB 15 (KY)
(1/1/2026)

How Are Fines Determined?

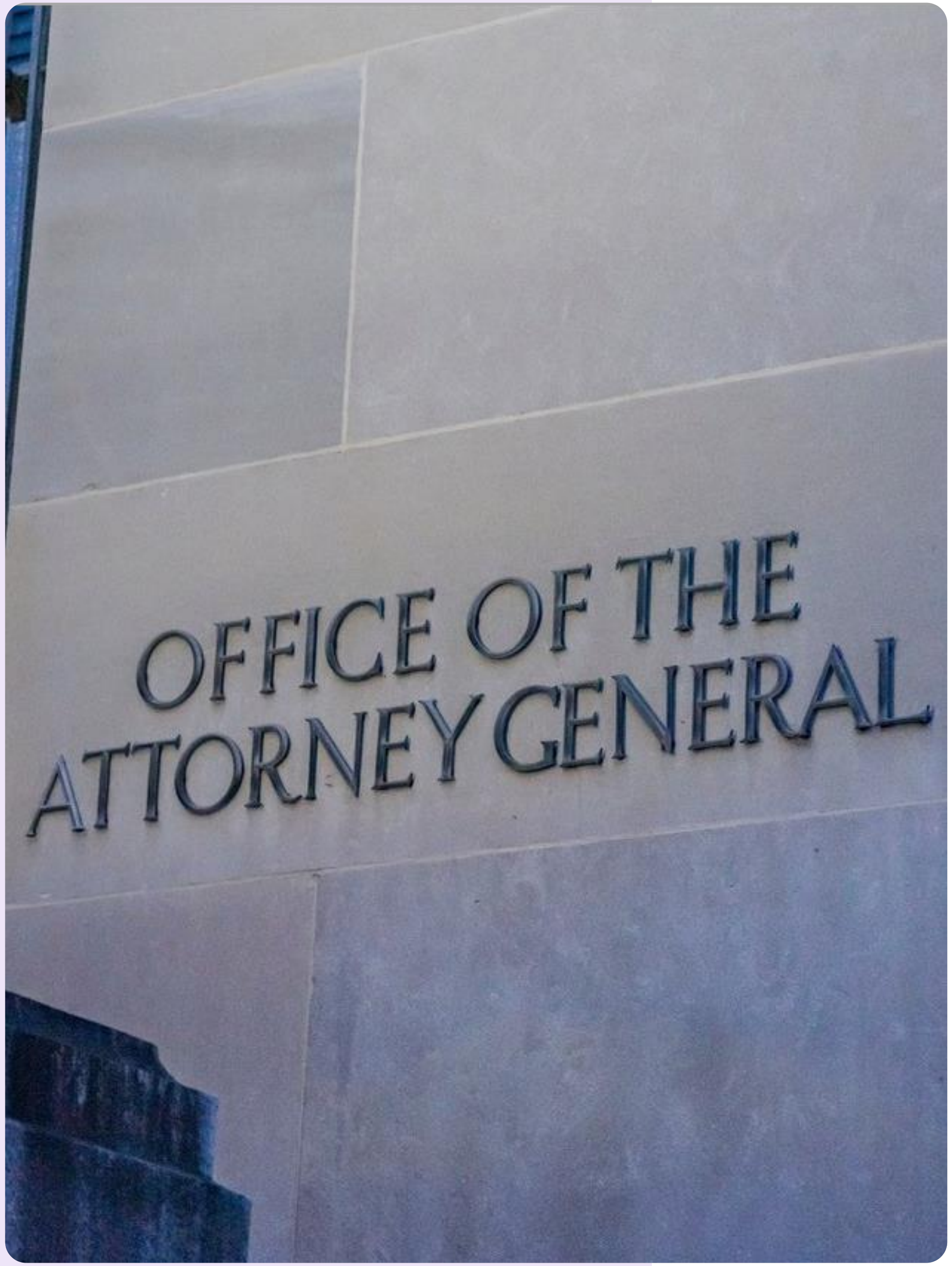
Calculating Fines

- Intentional vs. negligent violations
- Sensitive data and children's data
- One impacted person = one violation

Typical violation = $7,500

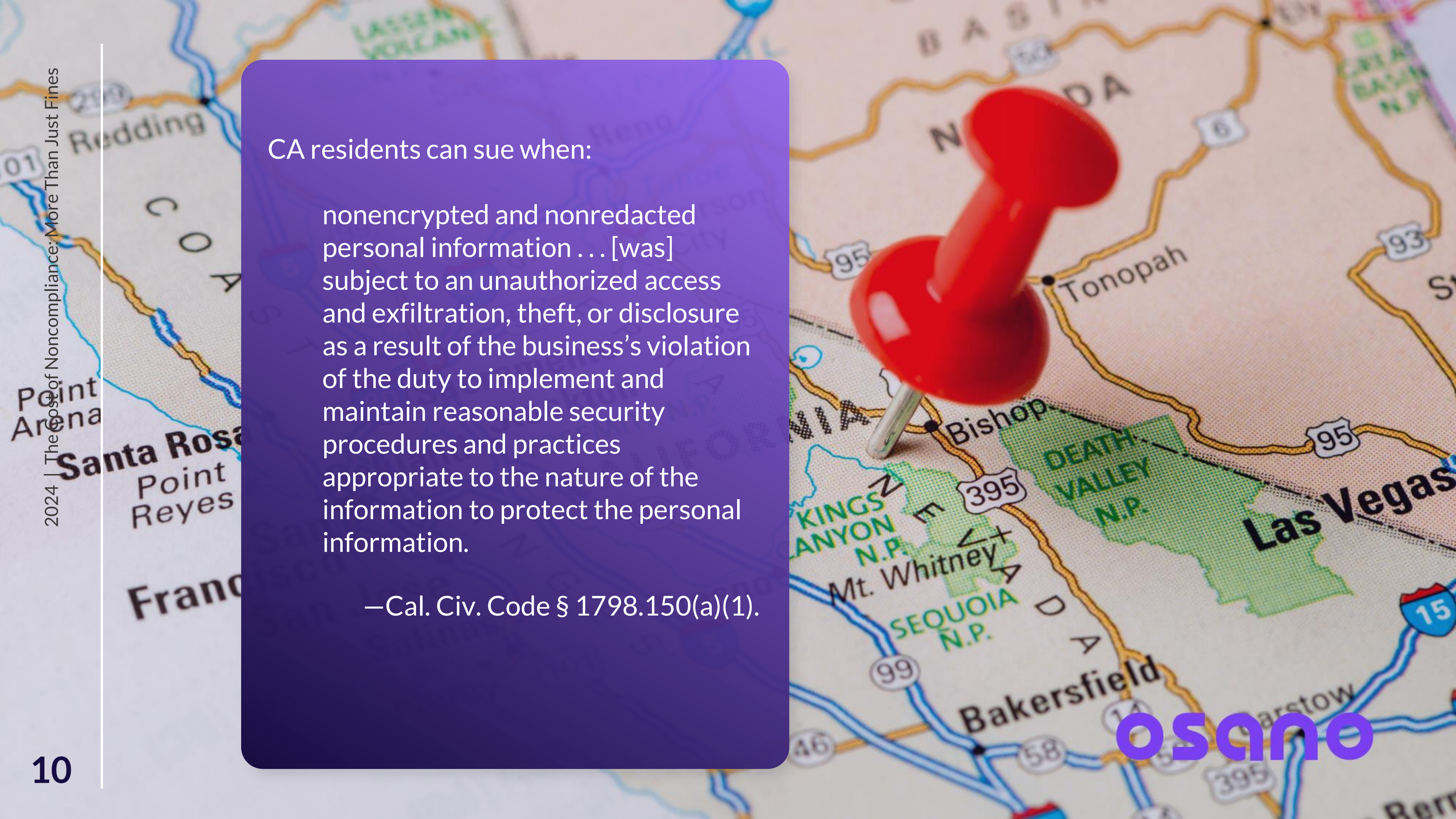
Exceptions:

- CO: up to $20,000
- CT: up to $5,000
- DE: up to $10,000
- MD: up to $10,000 and $25,000 per repeat violation
- MT: up to $10,000
- NH: up to $10,000
- NJ: up to $10,000 and $20,000 USD for subsequent violations
- TN: up to $15,000



Who Enforces the Law?

- State Attorneys General
- The California Privacy Protection Agency (CPPA)
- The Federal Trade Commission (FTC)
- Private citizens
  - Some laws, like the CPRA and the MHMDA, feature a private right of action.
  - Controversial component of the (proposed) APRA.
  - VT's proposed data privacy law was recently vetoed over this issue.



CA residents can sue when:

> nonencrypted and nonredacted personal information . . . [was] subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information.
>
> —Cal. Civ. Code § 1798.150(a)(1).

Cure Periods by State

None	California (AG/CPPA Discretion)								
30-Day	Virginia (no sunset)	Utah (no sunset)	Texas (no sunset)	Oregon (sunsets 1/2026)	Nebraska (no sunset)	New Jersey (sunsets 6/15/2026)	Indiana (no sunset)	Kentucky (no sunset)	Minnesota (6/31/2026)
60-day	Colorado (sunsets 1/1/2025)	Connecticut (sunsets 12/31/2024)	Montana (sunsets 4/1/2026)	Delaware (sunsets 1/1/2026)	New Hampshire (sunset 1/1/2026)	Tennessee (no sunset)	Maryland (4/1/2027)		
90-Day	Iowa (no sunset)								

Costs Beyond Fines

Poor data privacy practices incur additional costs beyond just fines for violations

01

Entering "firefighting mode"

- Receiving notice from AG
- Hearing of investigative sweep

02

Data breaches

- Poor privacy practices increase risk by 80%
- More data, greater impact

03

Loss of consumer trust

- 48% of consumers have stopped buying or using a service over privacy concerns

04

Weaponization of subject rights requests

- Vexatious requests intended to gum up operations
- Fishing expeditions

CCPA Enforcement Actions

Case	Beauty Retailer	Food Delivery Platform	Mobile Game Developer
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	Collected and shared children's data without parental consent in mobile app game via third-party SDKs
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 Once data was shared, it was difficult to "unshare"	Need for SDK governance: It's easy to overlook the tracking technologies in mobile SDKs
Cure period	Offered, violations not cured	Offered, violations not cured	Not offered
Penalty	**$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.*	**$500K + injunctive measures** *Comply with regs, not sell PI of children w/out opt-in consent, provide notice, provide neutral age entry screen, appropriately configure SDKs, implement an SDK governance framework, annual reports to AG.*

More Recent Enforcement Actions

FTC

- 4/11/24: X-Mode Social, Inc./Outlogic settles with FTC over sale of sensitive personal information.
- 2/22/24: Avast Limited banned from selling browsing data, ordered to pay $16.5 million.
- 5/20/24: Blackbaud, Inc. ordered to adhere to data minimization, transparency principles post-breach.

California

- 9/14/23: Google settles Cal. AG action for $93,000,000 action alleging that Google tracked location data without consent.
- 6/13/24: Blackbaud resolves Cal AG action for $6,750,000 alleging that Blackbaud failed to implement reasonable data security procedures, resulting in data breach.

New Wave of Litigation Targeting Tracking Tech

- Session replay software
- Wiretap Act and/or California Invasion of Privacy Act (CIPA)
- Video content on websites: tracking pixels (e.g., Facebook/Meta pixels) and video content = unlawful sharing of video viewing history in violation of Video Privacy Protection Act (VPPA)
- Chat widgets: alleged third-party interception of chat messages communicated to website
- Pixels and sensitive data: Class action *In re Meta Pixel Healthcare Litig. (ND. Cal.)*

Video Privacy Protection Act (VPPA)

- Prohibits the disclosure of information about consumers' consumption of video content without consent
  - Informed and in writing; separate and distinct from any other legal or financial obligations of the consumer
  - At the time disclosure is sought or given in advance for a set period of time, not to exceed two years or until withdrawn, whichever is sooner
  - Consumer is provided an opportunity, in a clear and conspicuous manner, to withdraw "on a case-by-case basis" or to withdraw "from ongoing disclosures," at the consumer's election
- "A video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider shall be liable to the aggrieved person"
- Commonly triggered by use of Meta pixel
- Actual, statutory ($2,500), punitive damages, attorneys' fees

$2.6M

Flosports

8/23/23

$5M

Boston Globe Media

9/8/23

$6M

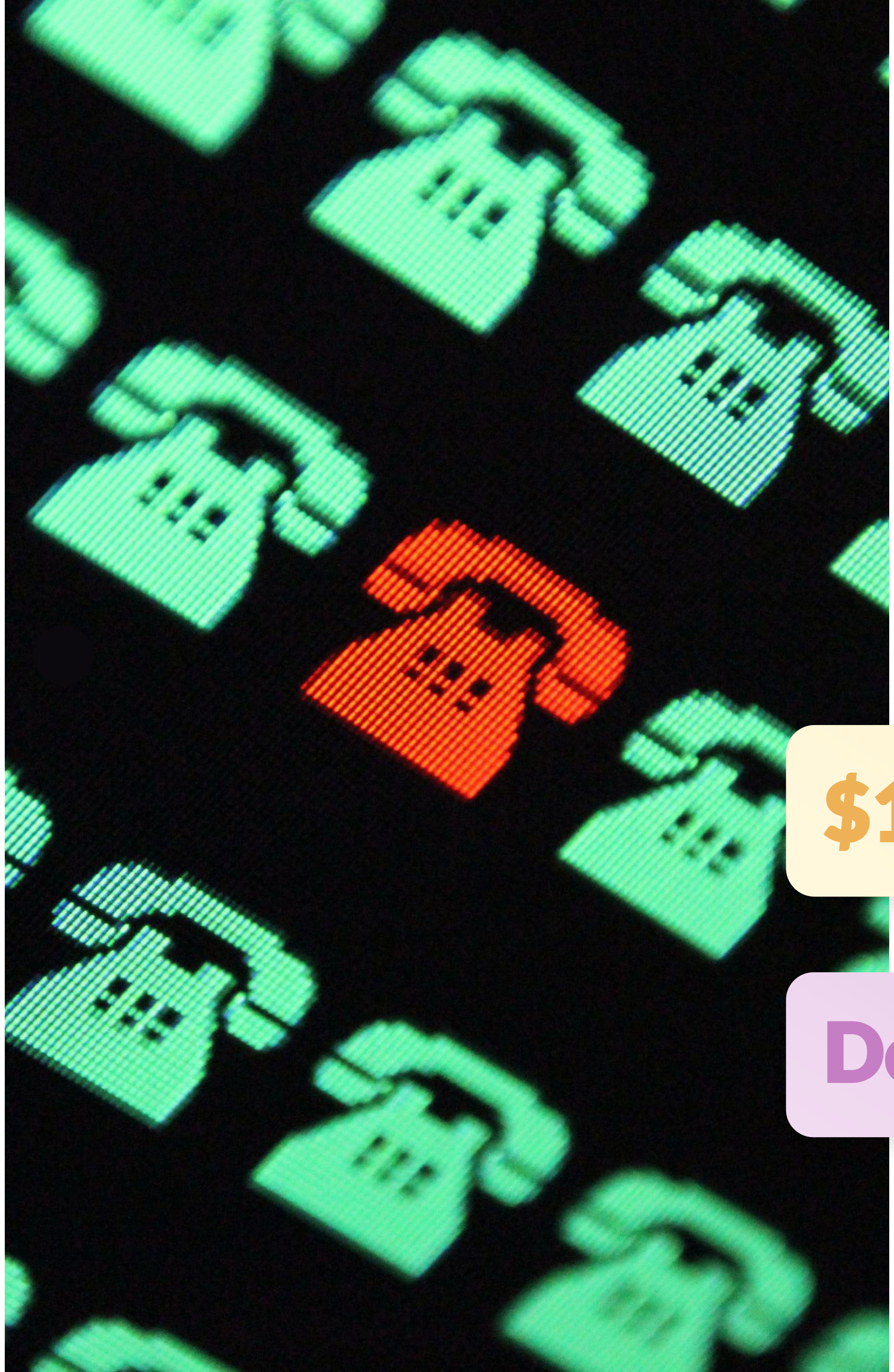
Fandango

12/4/23

$7.25M

Military.com

2/9/24



Wiretap Laws

- Wiretap Act (18 U.S.C.A. § 2511)
  - to intentionally intercept or procure any other person to intercept any wire, oral, or electronic communication
  - Key limitation: single party consent
- California Invasion of Privacy Act (Cal. Penal Code § 631) (CIPA)
  - “willfully and without the consent of all parties”
  - Aiding and abetting liability

$13M GoodRX settles FTC enforcement action alleging it shared sensitive health data through use of pixels and other tracking technologies in violation of Wiretap Act

Denied June 18, 2024, Court denies motion to dismiss class action against Google, HR Block, TaxAct for sharing tax info via Google Analytics tracking pixel

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?

Practical Advice for Compliance

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.

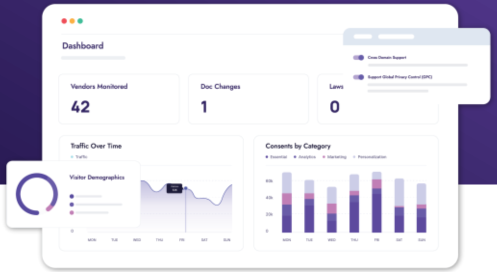
5. Assess Your DSAR Workflow

- 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

Stay In Touch and Learn More!



Dashboard

Vendors Monitored 42

Doc Changes 1

Laws 0

Cross Domain Support

Support Global Privacy Control (GPC)

osano

Schedule a Demo

Check out the Osano Blog

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/ACtQeZ3NST

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