

Webinar: Preparing for New State Privacy Laws: Key Requirements and Compliance Tips

Events

January 12, 2023

Gunderson Dettmer hosts the Preparing for New State Privacy Laws: Key Requirements and Compliance Tips Webinar. The webinar discussed the California Consumer Privacy Act (CCPA) and the European Union's General Data Protection Regulation (GDPR). Currently, several states have passed privacy laws similar to the CCPA and the GDPR. Gunderson Dettmer partner Anna Westfelt and associate Frida Alim and Cecilia Jeong led the webinar to share insights on how to prepare for the new laws and information about requirements, consumer rights, and non-compliance penalties.

Key Takeaways from this event include

- In 2022 five states passed comprehensive privacy laws and 27 states considered privacy bills.
 - January 1, The Virginia Consumer Data Protection (VCDPA) and the California Privacy Rights Act (CPRA) went into effect.
 - July 1, enforcement of the CPRA will begin, the Colorado Privacy Act (CPA) and the Connecticut Data Privacy Act (CTDPA) will come into effect.
 - December 31, the Utah Consumer Privacy Act (UCPA) will come into effect.

- The new laws are inspired from the California Consumer Privacy Act and the EU General Data Protection regulation.
- Compliant Tips:
 - Document compliance before an alleged violation.
 - If a state privacy law does not apply to you, document why.
 - Provide evidence of reasonable security.

Key Compliance Considerations

- “Sensitive Personal Information” under the CPRA includes a Social Security Number, passport, and proof of finances.
- Each of the privacy laws imposes obligations surrounding targeted advertising or “sharing” and “selling” under the CPRA.
 - Targeted advertising or “sharing” definition: Sharing personal information with another entity for the purposes of targeting advertising to a consumer based the consumer’s activity across businesses, distinctly-branded websites, applications, or services.
 - “Selling” definition: Sharing of personal information in return for monetary or other valuable consideration.
- Nearly all states have requirements when conducting a risk assessment. This occurs when legislatures or regulators view processing as high risk to the privacy of consumers or the security of their data: Data Protection impact Assessments (DPIAs).
- Each law requires specific language in processor/service provider contracts (data processing addenda, or “DPAs”).

Practical Compliance Steps

- Conduct a gap assessment
- Inventory and update data related documents
- Assess your processing activities
- Prepare to comply with consumer requests

- Update your public facing policies
- Consider technical solutions
- Implement a data retention policy
- Assess your data security measures

TRANSCRIPT

Event Information

Online

Related People



Anna C. Westfelt

PARTNER

P +1 650 463 5367



Frida Alim

ASSOCIATE

P +1 415 801 4921



Cecilia Jeong

ASSOCIATE

P +1 646 490 9094

Related Services

Data Privacy

Employment & Labor

Featured Insights

CLIENT NEWS

Brazilian Carbon Capture Company Mombak Announces \$30M Financing

CLIENT NEWS

Africa B2B OmniRetail Announces \$20M Financing

CLIENT NEWS

Glacier Announces Series A Financing to Expand Robot Recycling Fleet

CLIENT NEWS

Dataminr Announces \$100M Investment Led by Fortress Investment Group

CLIENT NEWS

Omnidian Announces \$87M Series C for Renewable Energy Performance

INSIGHTS

Splitting the Pie: How Savvy Founders Divide Ownership and Navigate Other Founder Equity Decisions

CLIENT NEWS

Chainguard Announces \$356 Million Series D Led by Kleiner Perkins and IVP

INSIGHTS

Client Insight: California AI Transparency Act

INSIGHTS

Client Insight: Prepare for BE-10 Benchmark Survey of US Direct Investment Abroad

INSIGHTS

Tech Brew Interviews Aaron Rubin in “Where the legal battle stands around copyright and AI training”

CLIENT NEWS

Latin America Fintech Belvo Announces \$15M Funding

INSIGHTS

Legal 500 Country Comparative Guides 2025: Venture Capital (Singapore)