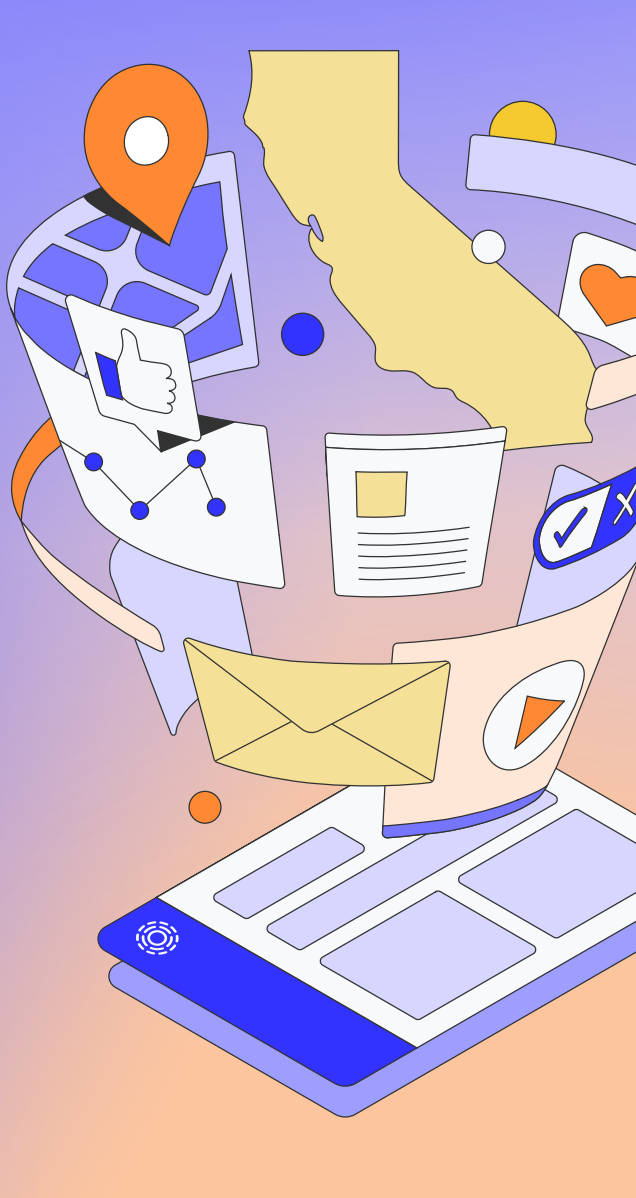
Transcend

Gartner Peer Insights

Is Your Company Ready for Technical Privacy Laws?

California continues to lead the charge on increasingly technical privacy regulations in service of greater consumer privacy protections. The upcoming California Privacy Rights Act (CPRA) expands the existing California Consumer Privacy Act (CCPA)—marking the state's next jump forward.

As CPRA's January 1st, 2023 enforcement date looms closer, companies are pushing to fully understand the law's requirements and ensure they have the resources and tools to comply. This report checks in with tech leaders on overall CPRA readiness and remaining compliance challenges.



Some key areas we explored:

01
How aware are leaders of the full scope of changes introduced by CPRA?

02
An expansion of the right to opt out of the sale of personal information—what are the compliance implications of the CRPA's more robust Do Not Share standard?

03
Are businesses' current privacy programs, including processes, data inventories, and technical resources, enough to support compliance with these new requirements?

04
Are companies prepared for potential consequences now that California has formed a dedicated Privacy Protection Agency charged with enforcing the law?

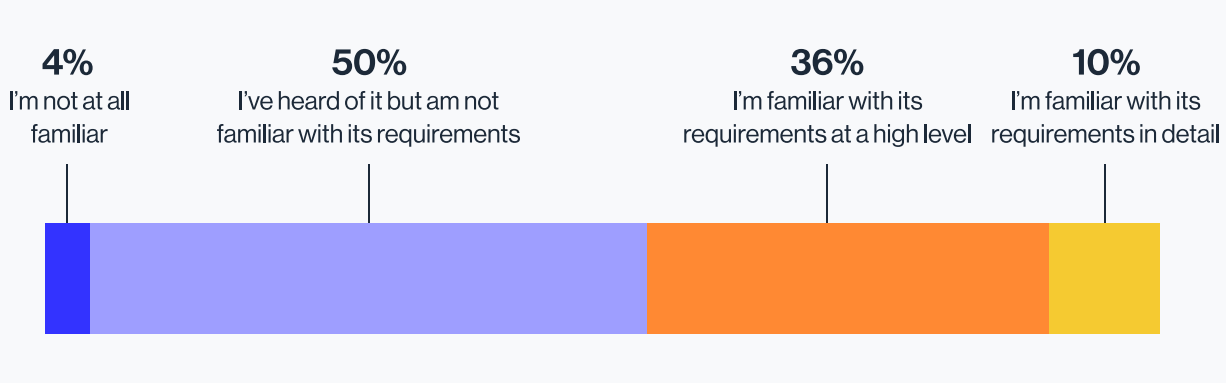
To answer these questions, Gartner Peer Insights and Transcend surveyed 100 engineering and legal leaders at companies that do business in California or collect personal information from California residents.

Data collection: April 9 - May 30, 2022 | Respondents: 100 engineering and legal leaders

Most surveyed (90%) are still trying to fully understand CPRA's new requirements, are not confident their organization will be compliant by the January 1, 2023 deadline, and are considering investing significant resources to improve their privacy infrastructure.

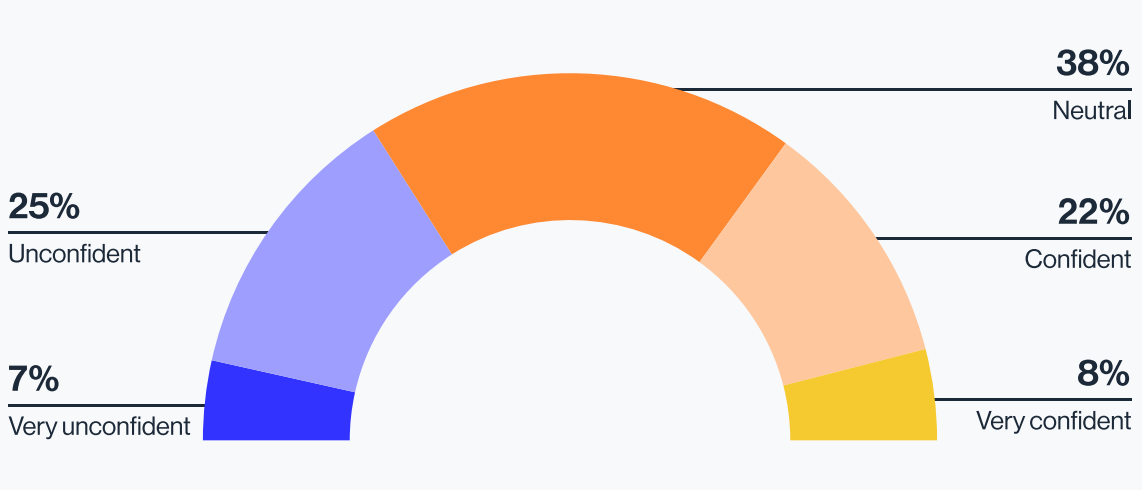
Just 10% of those sampled consider themselves well versed in CPRA's new requirements.

How familiar are you with the California Privacy Rights Act of 2020 (CPRA) which amended the existing California Consumer Privacy Act of 2018 (CCPA)?



Only 30% are confident or very confident that their organization will be fully compliant with CPRA before the January 1, 2023 deadline.

How confident are you that your company will be fully CPRA (California Privacy Rights Act) compliant by the January 1st, 2023 deadline?

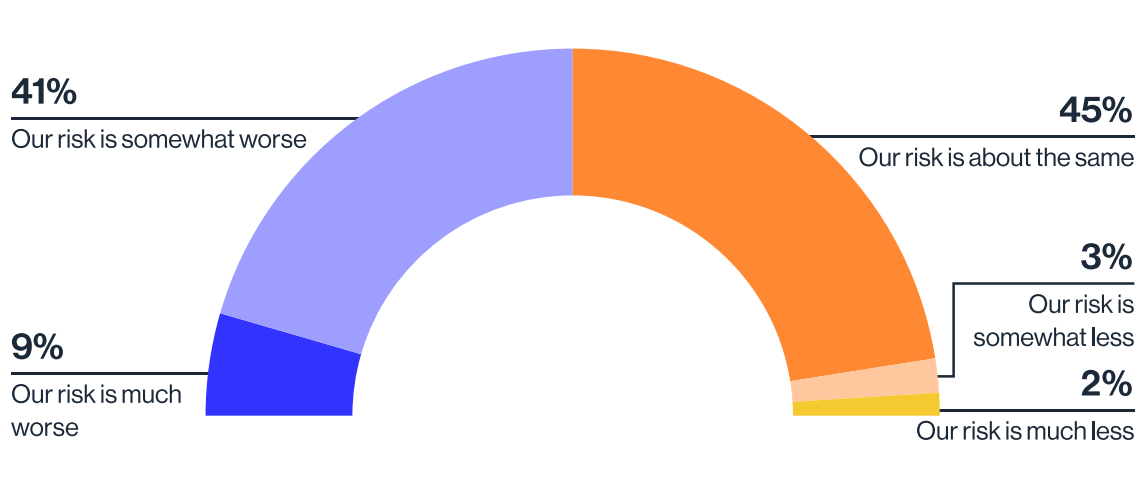


CPRA's expanded Do Not Share opt out requirements add significant new complexities with 50% reporting it increases their compliance risk.

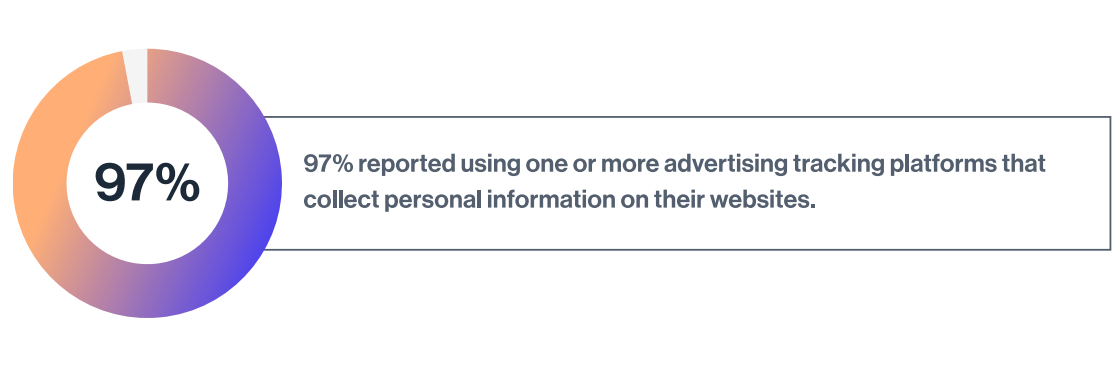
Only a handful have in-house engineering bandwidth to fully build technology needed to pass opt-out requests to downstream vendors and ad platforms as required under the updated law.

Business leaders are wary of the law's broader opt-out requirements which are aimed in part at companies that run targeted advertising campaigns — many see it increasing their compliance risk.

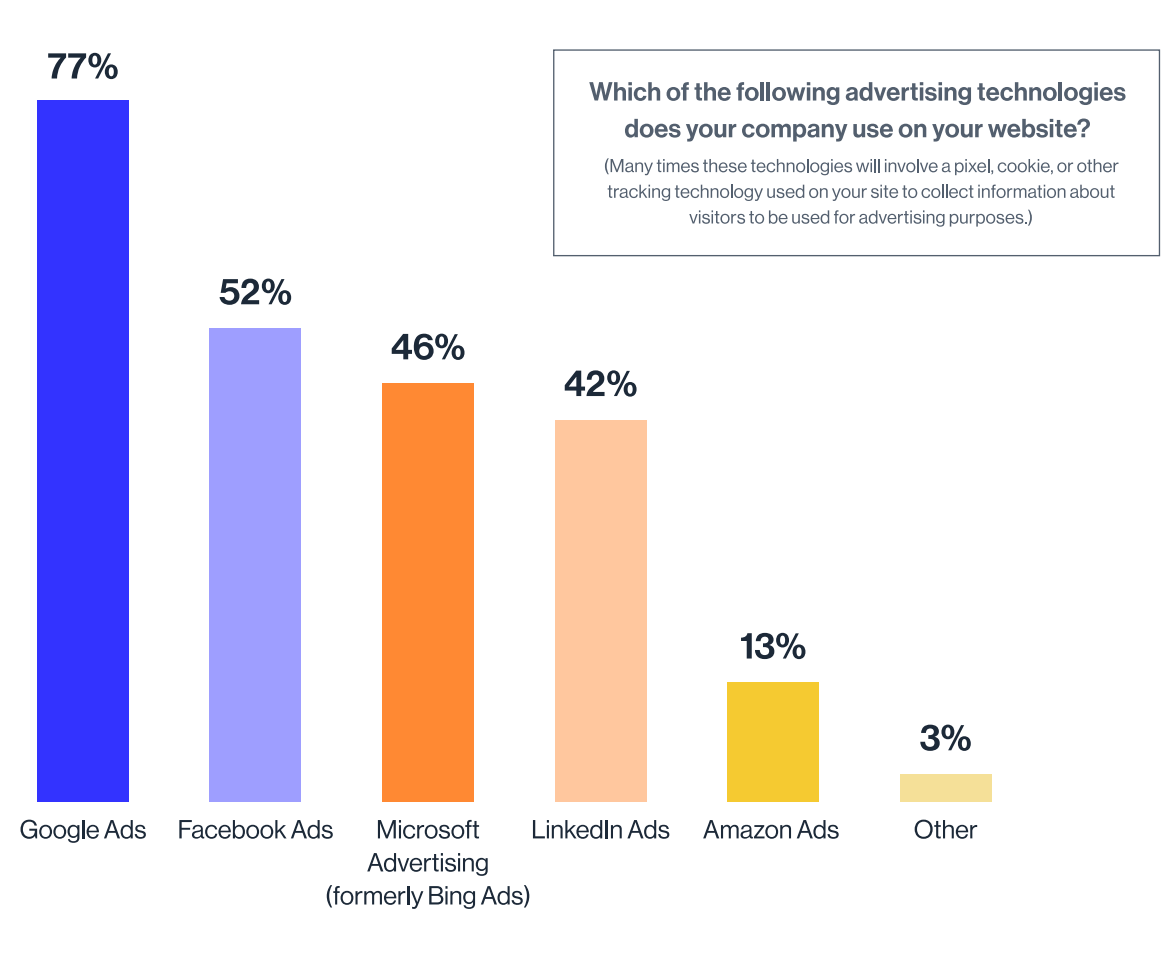
How does CPRA's change from a "Do Not Sell" opt-out requirement to a more broad "Do Not Sell OR Share" opt-out requirement impact your company's compliance risk?



97% reported using one or more advertising tracking platforms that collect personal information on their websites — Google Ads is the most widely used platform (77%), followed by Facebook Ads (52%)"

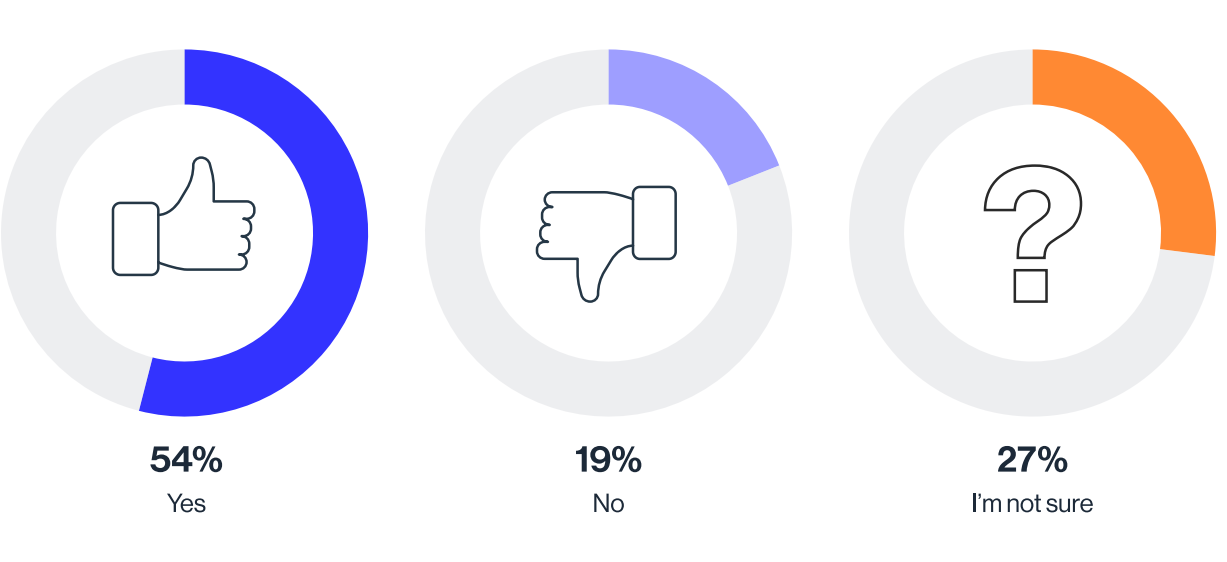


Which of the following advertising technologies does your company use on your website?
(Many times these technologies will involve a pixel, cookie, or other tracking technology used on your site to collect information about visitors to be used for advertising purposes.)



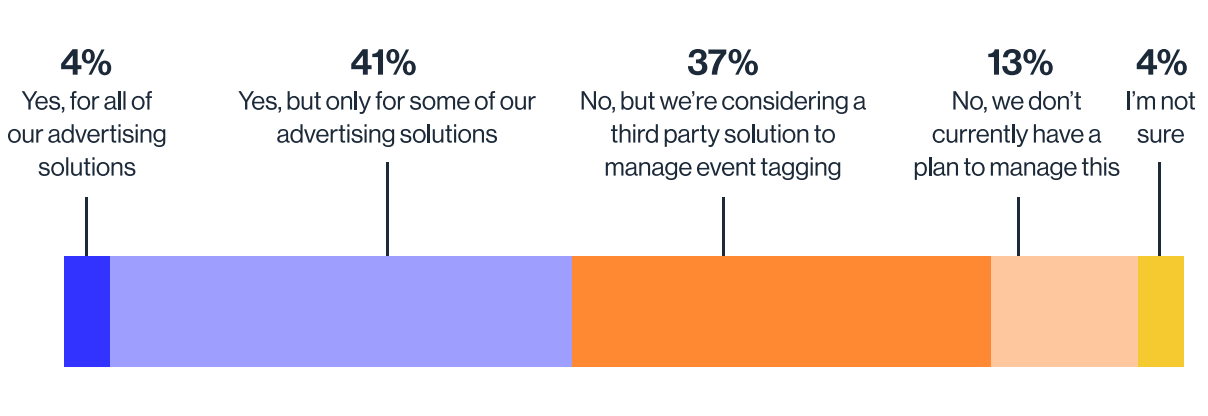
Despite the vast majority reporting they use targeted advertising technology on their websites, 46% of respondents either have not or are not sure if they have implemented event tagging to pass "Do Not Sell or Share" requests directly to each ad platform.

Have you implemented event tagging so that you're passing website visitors' "Do Not Sell or Share" requests through to your advertising platform(s)?



Some respondents (41%) are attempting to implement Do Not Share using in-house resources, but only 4% report having the engineering bandwidth to build and maintain compliance across all their ad-tech. Over one third (36%) are already considering external tools to help achieve compliance.

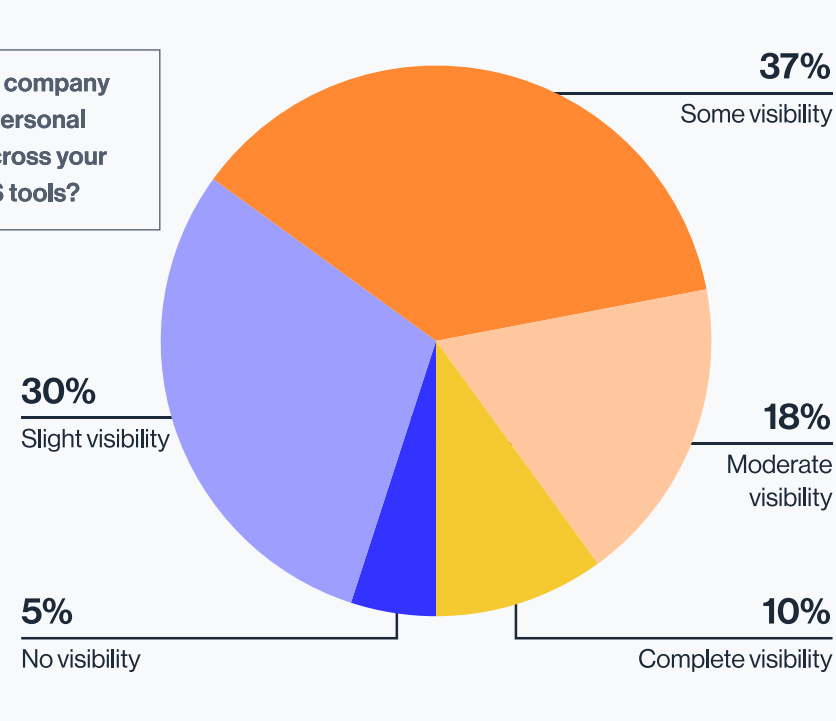
Do you have the engineering sprints reserved to implement full compliance with Do Not Sell or Share event tagging for each advertising solution you use? (n=46)



Internal visibility into personal data collected, stored, and subject to California's privacy regulations is patchy, and most companies lack automation to scale their privacy programs to meet the new regulatory burden.

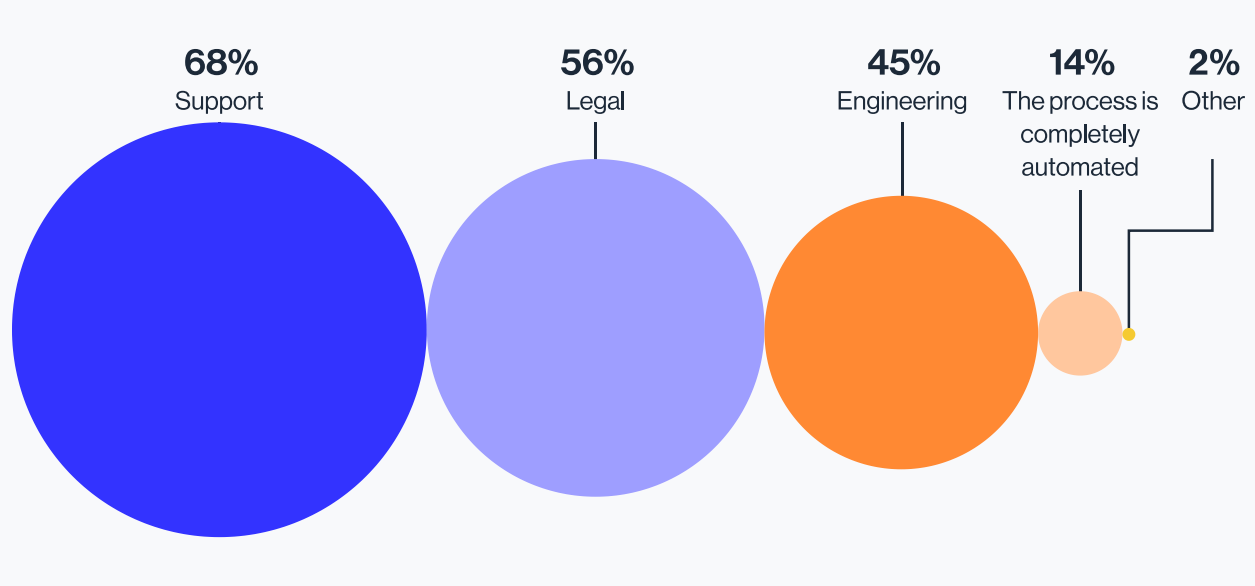
Only 10% of respondents have the full data visibility to comply with CPRA requirements.

How much visibility does your company have into everywhere that personal information is being stored across your technology stack and SaaS tools?



Only 14% of companies have fully automated workflows to handle privacy requests and are instead dependent on manual workflows to scale with demand brought by new regulations.

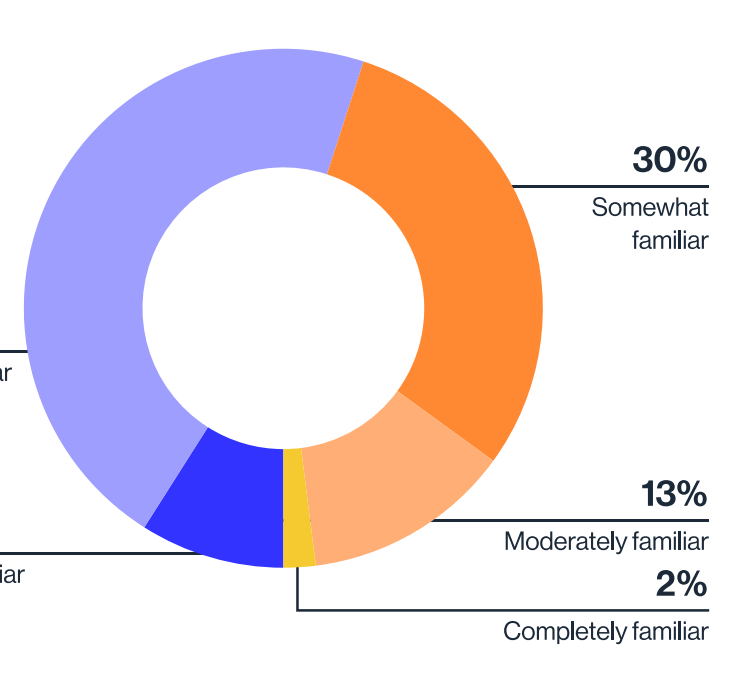
Who or what team is currently (or will be) responsible for facilitating personal information corrections that consumers submit?



The majority of leaders surveyed aren't yet familiar with the new fines established by CPRA and are considering investing significant resources to improve their privacy infrastructure.

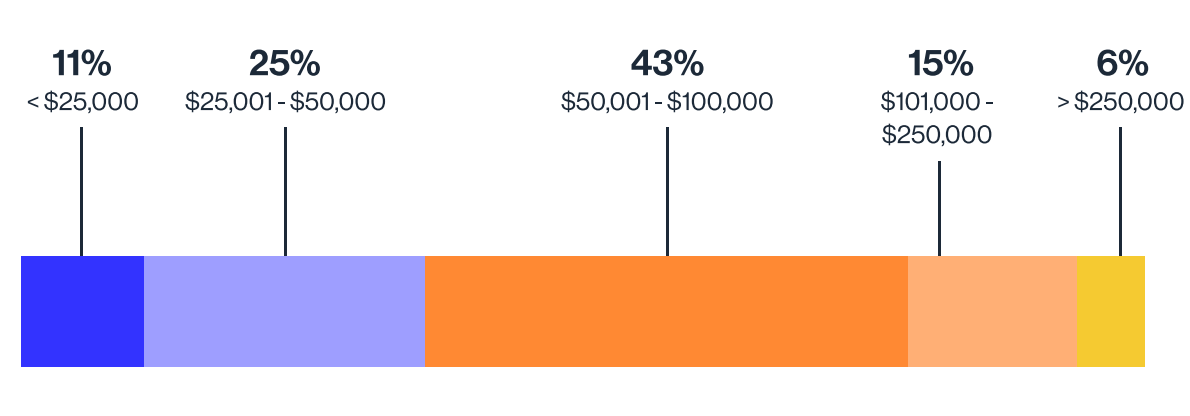
Only 2% of those sampled are completely familiar with the fines and penalties that the California Privacy Protection Agency, the new enforcement body established by CPRA, can levy against companies that violate privacy laws.

How familiar are you with the fines and penalties that the California Privacy Protection Agency can use against companies found to violate privacy laws?



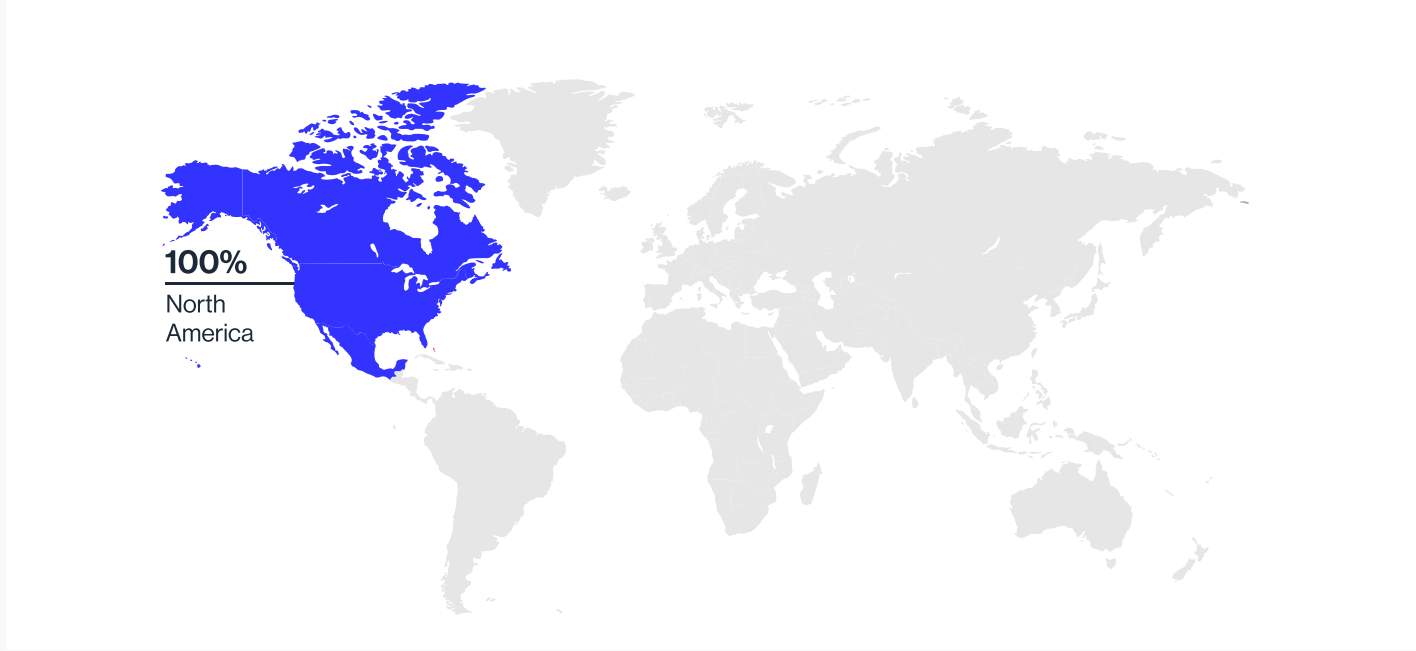
Over half of respondents (58%) are willing to invest between $50,001 and $250,000 to reduce their risk of noncompliance with the new laws and regulations.

CCPA and CPRA fines vary between $2500 and $7500 per violation. How much is your company prepared to invest in technology or resourcing to reduce the risk of noncompliance?

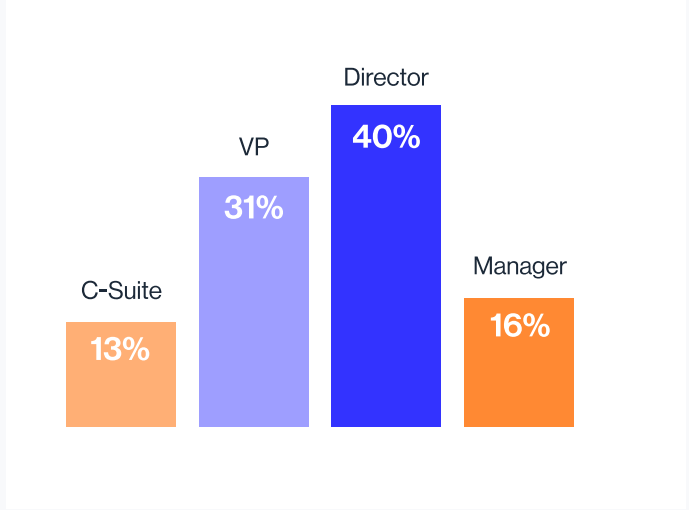


Respondent Breakdown

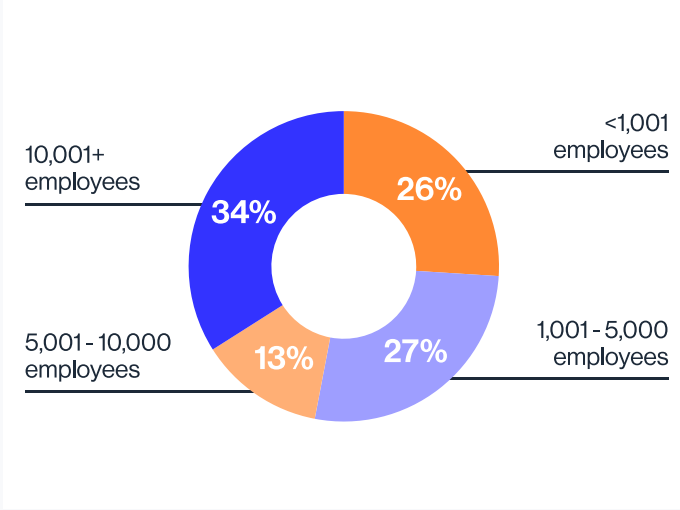
Location



Title



Company Size



Transcend is making it simple for companies to comply with increasingly complex privacy laws.

Personal data is disorganized, hard to spot, and moves between many systems. That makes offering data rights and complying with modern privacy laws very hard for companies. Transcend offers a single system that maps privacy requirements to your company's tech stack and automates time-consuming privacy tasks. From automatic cataloging of advertising tech to out-of-the-box Do Not Share event tagging and privacy request fulfillment, Transcend helps companies like Robinhood, Patreon, and Clubhouse reduce their compliance risk, save resources, and give their users control over their personal data.

Learn more at transcend.io

Transcend

Gartner

Source: Gartner Peer Insights, Readiness Privacy Regulations survey