JANUARY 30, 2026 | AI/TECHNOLOGY, PRIVACY & DATA SECURITY

Privacy Notices Explained: When a Policy Is Required and When It Is Not Enough Consumer Privacy Thresholds, Point-of-Collection Disclosures, and Employment Data Considerations

By Darius Rohani-Shukla

Publishing a website privacy policy is now standard practice. But assuming that a single, generic policy covers everything is inherently risky. In reality, privacy obligations can arise from several directions: baseline online notice expectations when you collect personal information through a website or app, comprehensive state consumer privacy laws that apply once you cross certain thresholds, and separate requirements that apply in the employment context.

In many cases, meeting those obligations is not just a matter of maintaining a policy in the footer. It also requires the right disclosures at the moment data is collected, whether that is through cookies and tracking technologies, a signup form, a checkout flow, or an application portal. Recruiting and workplace data add another layer. Applicant information, employee monitoring, biometrics used for timekeeping or access control, and automated hiring tools can each trigger standalone notice obligations that a consumer-facing privacy policy does not address.

This blog summarizes when a privacy policy is legally required, when additional point-of-collection disclosures are appropriate, and how consumer and workforce requirements can overlap.

Online Collection and Baseline Privacy Obligations

If your website collects personal information, even through basic contact forms, newsletter signups, account creation, analytics identifiers, or advertising pixels, you should plan to post a public-facing privacy policy that accurately describes what you collect, how you use it, and who you share it with.

California's CalOPPA is one reason many organizations treat this as a baseline for commercial websites that collect personal information from Californians. CalOPPA is California's online privacy notice law, requiring operators of commercial websites and online services that collect personal information from California residents to post a privacy policy. It is also a practical baseline because other state privacy laws, sector-specific federal

rules, and consumer protection enforcement all reward clear, accurate public disclosures about data practices.

Crossing the Threshold: When State Consumer Privacy Laws Apply

Many states now have comprehensive consumer data privacy laws, but unlike baseline online notice rules, these laws do not apply to every business by default. Instead, they generally apply only once a business crosses defined thresholds tied to revenue, the scale of consumer data processing, and in some cases the sale or sharing of personal data. California and Virginia are useful reference points because their frameworks illustrate the kinds of triggers other states often adopt, even if the specifics differ.

California (CCPA/CPRA). A for-profit business is generally covered if it meets any of these thresholds:

- Gross annual revenue over $25 million (adjusted for inflation)
- Buys, sells, or shares the personal information of 100,000+ California residents or households
- Derives 50%+ of annual revenue from selling Californians' personal information

The California Privacy Protection Agency lists the inflation-adjusted revenue threshold as $26,625,000.

Virginia (VCDPA). Coverage generally turns on:

- Controlling or processing personal data of 100,000 consumers in a calendar year, or
- 25,000 consumers if more than 50% of gross revenue is derived from the sale of personal data

When these laws apply, compliance typically goes beyond publishing a privacy policy. Covered businesses are generally expected to provide required disclosures about data collection, use, and sharing, and to operationalize consumer rights requests within statutory timelines. Depending on the state, those rights can include access, deletion, correction, and opt-outs that may cover targeted advertising or "sale." Businesses also typically need contracts and procedures that support those obligations across vendors and internal systems.

Penalties are a key reason the "threshold moment" matters. In California, the CPPA's inflation adjustment identifies 2025 administrative fine amounts of up to $2,663 per violation and up to $7,988 per violation for intentional violations (and certain violations involving minors). (cppa.ca.gov) In Virginia, civil penalties can be up to $7,500 per violation, enforced by the Attorney General.

Finally, this is a fast-moving, state-by-state patchwork. New state laws continue to take effect and existing laws are amended over time, and requirements can differ materially across jurisdictions, including definitions of "sale," treatment of sensitive data, opt-out mechanics, and required notice content.

When Candidate and Employee Data Triggers Notice Obligations

Workforce data can trigger notice obligations as well. It can be easy to miss because employee and applicant information is collected and used in different systems and contexts than customer data. Many state consumer privacy statutes define "consumer" in a way that generally excludes people acting in an employment context, and Virginia is explicit on this point.

California is the key exception. The CCPA/CPRA framework treats California residents as covered, including employees and job applicants. There was real back-and-forth for a period because workforce obligations

evolved over time, but the practical drafting point today is that the California Attorney General has signaled workforce compliance is an enforcement priority. For CCPA-covered businesses, this is why it is common to maintain a separate applicant or workforce notice in addition to a public website privacy policy, and to be prepared for rights workflows where required.

Separately, a number of employment-specific laws impose notice or policy requirements regardless of whether a business meets consumer privacy law thresholds, which is often where employers are caught off guard. These obligations are triggered by particular workplace practices, not by revenue or data-volume tests.

Common examples include Illinois' Biometric Information Privacy Act (BIPA), which requires a publicly available written biometric policy with a defined retention schedule and destruction guidelines; New York's electronic monitoring law, which requires notice upon hiring, employee acknowledgment, and workplace posting for covered monitoring activities by employers; and New York City Local Law 144, which imposes bias audit and advance notice requirements for certain automated employment decision tools.

A Practical Approach to Privacy Notices

Being thoughtful about who you are giving notice to, and when, is just as important as what the notice says. Privacy obligations do not always start and end with a public website policy. Depending on your data practices, you may also need point-of-collection disclosures. and separate applicant or workforce notices for recruiting, monitoring, biometrics, or automated decision tools. A practical approach is to map data flows by audience (visitors, customers, candidates, employees) and confirm your posted notices match what actually happens at each collection point. Please feel free to reach out if you would like to talk through any of these questions or want help confirming what notices and practices make sense for your specific setup.