

Data privacy basics – privacy policies

Most companies have an online presence, but not all include a privacy policy on their site. Determining when you need one and what the policy should contain is a fundamental matter that every company should consider as part of its formation.

When is a privacy policy needed?

Laws in several states require websites, mobile applications, and other online services that collect personal information to have a privacy policy posted on the respective online service. Although the precise scope of content varies based on the law, in general these laws require the privacy policy to describe what Personal Information the company collects, and how it will use and disclose that data. The laws require disclosures about how third parties, such as advertising networks or others, may collect personal information about consumers who visit or use the website, app, or service. California law also requires that companies that share personal information with third party marketers make certain disclosures about their practices in their privacy policy and give consumers a way to request a list of the companies to whom their information has been disclosed.

In addition to the above-mentioned state laws focused specifically on the maintenance of a privacy policy, several states have adopted laws providing comprehensive data privacy rights for residents of their states. One example is the California Consumer Privacy Act (CCPA). A key component of these laws, including the CCPA, is providing a detailed notice to the consumer, among other requirements, of the consumer's rights. In general, the threshold for being subject to the comprehensive state privacy laws is greater (e.g., revenue or amount of data collected) than the laws pertaining specifically to privacy policies, which apply on a broader base.

In addition, the Federal Trade Commission (FTC) has issued best practice guidance for companies that handle consumer personal information to provide greater transparency into their information collection practices through clear and meaningful privacy notices.

Are there special rules for a privacy policy for my company's mobile app?

As stated above, mobile applications—not just websites—that collect personal information should maintain a privacy policy available within the app. There are specific considerations for mobile applications. Specifically, both the FTC and the California Attorney General have released best practices guidance for mobile privacy, recommending, among other things, that companies make a short-form version of their privacy policy accessible within a mobile app. Companies also should obtain specific consent to collect and/or access certain types of data (e.g., precise location, health, biometrics, as well as to access contacts, photos, among other data elements) via the mobile app. Further, California law specifically requires that app providers make available a privacy policy from within the mobile app, and applies to any company that collects personal information (which could include online identifiers such as IP address) through a mobile app or online service.

Takeaways

Most companies that handle consumer data – whether as a service provider or a data owner – should post a privacy policy online and through any mobile apps. It is important to note that a privacy notice also should comply with the content requirements of state laws and FTC best practice.



ACCELERATE

DLA Piper is a global law firm operating through DLA Piper LLP (US) and affiliated entities. For further information please refer to www.dlapiper.com. Note past results are not guarantees of future results. Each matter is individual and will be decided on its own facts. Attorney Advertising. Copyright © 2025 DLA Piper LLP (US). All rights reserved.