



## LEGAL UPDATES

# Privacy and Security Basics – Do's and Dont's

As more and more states implement privacy laws, businesses must stay up to date with them and continuously address their data privacy and security practices.

01/10/2023 | 4 minute read

As more and more states implement privacy laws, businesses must stay up to date with them and continuously address their data privacy and security practices. Even if a business is not subject to any of the new state laws, the Federal Trade Commission has wide latitude in enforcing businesses and their privacy practices. If a business collects personal information, it must have a proper privacy policy that accurately reflects its business practices. Here is a short list of privacy and security related do's and dont's businesses should follow.

- **Do Update Privacy Policies.** Even if your company previously was not subject to certain laws, such as the EU's General Data Protection Regulation, or California's California Consumer Privacy Act as modified by the California Privacy Rights Act (collectively, the "CCPA"), you should reevaluate your company's privacy policy at least annually. If any of your data practices have changed or any of the parameters that could bring you under the purview of certain laws have changed, it is time to reassess and update your policies. For example, ask if any of the following have changed: the types of data you collect, revenues, your target marketing audiences, or actual customer numbers. Additionally, new state laws are coming into effect at regular intervals. Regulators are issuing new and updated regulations, which may bring new requirements and cases and public settlements are instructive on where businesses went wrong. Privacy policies are not a "set it and forget it" document and must be seen as a living document that must be updated to reflect reality or otherwise face the risk of an enforcement action. Indeed, it is best practice to update privacy policies on any significant change and certain laws, such as the CCPA, actually require annual updates.
- **Don't Ignore Employee Privacy.** Certain privacy laws now also apply to data collected from individuals in the employment context, including from employees, contractors, and board members. Companies must have separate privacy policies that specifically address this type of employment data, in addition to the data from individuals companies usually consider e.g. website users and consumers. Employees have further rights to access data, ensure inaccurate data is corrected and to have data deleted. Companies will need to adjust their employee handbooks, internal policies, and consider notes they

## Related People

### Chiara Portner, CIPP/US

Partner

Redwood Shores

650.804.7672

[chiara.portner@lathropgpm.com](mailto:chiara.portner@lathropgpm.com)

## Related Services

[Data Privacy & Cybersecurity Compliance](#)

[Corporate & Business](#)

[Labor & Employment](#)

[Real Estate & Development](#)

## Related Sectors

[Retail & E-Commerce](#)

take and retain for hiring and review efforts.

- **Do Address Dark Patterns.** Dark patterns are aspects or features of a user interface designed to, or do indeed, confuse or manipulate the user or encourage the user to take a certain action that may not be in their best interest. For example, a dark pattern may exist if you see a cookie banner with two buttons: one button in a shaded or lighter color with the option to decline cookies (or manage cookie preferences) alongside a second more prominent, or brighter button to have the user consent to all cookies. If your interface choices draw an individual's eye to the less privacy protective choice, this is likely a problem. These practices deceive users and may have the effect of limiting their meaningful choices under applicable laws. The FTC and State Attorneys General are watching for dark patterns and bringing enforcement actions against companies for them.
- **Do Train Employees on Privacy and Security.** Make security, and training personnel on security a priority. We have seen multiple data breaches, in some cases of information that is considered sensitive, because an untrained employee fell victim to a phishing scam or other malicious scheme or what looked to be an innocent download or click. According to a recent study, the human element was the cause of 82% of security breaches in 2022. Having various security measures and policies in place is a first step. But, internal policies must be circulated and enforced, and employees should be kept abreast of and periodically trained (and tested) on evolving threats and changes in data security.
- **Do Address Data Retention.** To further mitigate risk, companies should implement a data retention policy that balances their different legal obligations to retain data with the need to minimize it. Whether it is employee, consumer, or customer data, know how long you are legally required to retain it and then destroy what should not or does not need to be retained. Many companies hoard data in case they might want to use it, without any current legal or business justification. In doing so, they substantially increase risks in the event of a data breach. The more data you have, the more you have to lose. Not only is there increasing risk of class actions with respect to data security breaches with laws such as the CCPA, which carry a private right of action (including class actions) with statutory damages, but State Attorneys General are also bringing enforcement actions against companies for failing to adequately secure data when such failure results in a security breach.
- **Don't Ignore Vendor Relationships.** State privacy laws include requirements that companies have certain contracts in place with contractors and service providers. Contracts must allow some level of due diligence for businesses to conduct due diligence to ensure compliance and security. Companies should update or implement a data processing agreement or addendum for each vendor, which agreement or addendum must contain specific language for vendors that qualify as service providers or contractors. State laws, such as the CCPA, even require specific language be included in contracts with third party vendors that are not processing data on behalf of a business and that use data for their own purposes.
- **Do Get Cyber Security Insurance.** Cyber security insurance is necessary these days, with more security breaches than ever before, and more breaches likely to come in a recession economy. The cost of security breaches and the reputational fallout can be significant and insurance coverage can mitigate the costs. It is important to keep in mind security should be a priority and insurance coverage may be at stake if a company chooses to ignore privacy and security regulations. Even for companies that do obtain insurance coverage, in the event of an incident, they could be left hanging if their insurers determine they were not sufficiently proactive in implementing privacy and security practices