# PUBLICATION

## Data Privacy Day 2020 – What Actions Businesses Can Take

**Authors: Alisa L. Chestler**
**February 2020**

**Happy Data Privacy Day! Today, January 28, is a day to raise awareness, foster dialogue, and empower companies to act to ensure proper privacy (and security) of all types of data and information.**

Data privacy, as a concept, deals with how information is used, as well as whether an organization has the legal right or proper permissions to use the information it obtains. Data security is an extension of privacy, and it relates to the protection of data, once collected, from unauthorized access or disclosure.

Data is everywhere, and it is valuable. Governments, businesses, and individuals maintain, retain, and share vast quantities of data. When individuals provide information about themselves, the recipients of that information have a responsibility to protect it – either entirely or to a specified degree. Unfortunately, not all businesses fully appreciate this responsibility. Further, many companies are oblivious, often unwittingly, to the extent of information they are collecting.

For example, when a consumer downloads a company's app on their smartphone or device and agrees to the privacy policy and terms-of-service agreement that goes along with the download, that app is gathering information, such as geolocations, browser data, stored contacts, microphone audio, photographs, etc., from the consumer's device. Much of this information may be unwanted or unnecessary for the company's purposes; however, it's still being collected by the company via the app, oftentimes without the company even realizing that the app is collecting the data. This is because app developers program apps to take on all sorts of information, simply because it's possible, even though they have not asked or been informed about what information a company actually wants or needs to track.

Unfortunately, there remains no comprehensive federal-level data protection authority or privacy legislation that regulates the overall collection and use of personal data in the United States. Instead, while various sector-specific data protections exist on a federal level,[1] the majority of data privacy and security regulations exist at the state level. And state-level requirements are multiplying rapidly. Following the California Consumer Privacy Act (CCPA), which went into effect on January 1, 2020, multiple states have enacted or proposed similar bills to protect consumers through comprehensive privacy and security legislation. With this piecemeal onslaught of new laws coming into effect so quickly, too many businesses fail to realize that, while they may not have any specific operations in California (or in the other states that have enacted similar legislation), the laws still apply to and impact them.

Companies bear the brunt of navigating this system of highly complex variations of laws related to data privacy and security. Doing so comes with a hefty price tag as well as a heavy administrative burden.

But, don't be dismayed: there are things you can do to ensure that your company is on the right track with respect to protecting its data!

Actionable steps for businesses include:

1. **Review your company's privacy policies and terms-of-service agreements.** Make sure they meet the legal requirements that are applicable to your company and industry. Verify that users or customers can easily understand what data is being collected and what is being done with it, and make sure that clear opt-in or opt-out processes are provided.

2. **Critically assess the data that your company collects and retains.** If your company is collecting unnecessary or unwanted information, update the processes of collection to appropriately limit the information that is obtained and retained.

3. **Map the data that your company collects.** You need to be able to track and manage the information that is being collected at all points in the process, including where it may end up in the future.

4. **Consider appointing a Data Officer who will be responsible for your company's legal compliance with a privacy and related issues.** This person should keep up-to-date with legal developments, news, and trends related to your company's and industry's specific data privacy needs, or work with competent counsel to help with this.

5. **Adopt a proactive mindset of responsibility when it comes to handling data.** Build for the future with privacy in mind instead of having to back-track to implement policies and protections as reactionary measures.

6. **Require multi-factor authentication – one of the best current defensive tactics to avoid a cyber incident.**

7. **Add levels of encryption for data and devices.** Enact and enforce policies that will help to avoid data breaches on a system-wide level.

8. **Obtain sufficient cybersecurity insurance protection.** If you don't have cybersecurity insurance, get it now. If you have coverage, make sure that your coverage is sufficient for your business needs. In addition, don't forget how cybersecurity coverage might intersect with other policies and coverage, such as business interruption and crime policies.

On this Data Privacy Day, it is important to consider and assess your company's data, and to learn about what information exists, how it is being used, and where it is going. Take proactive steps to ensure that the data that your business receives is known and accounted for, handled properly, and sufficiently secured. Now that you've got some actionable steps, you should feel empowered to ensure proper privacy and security of your company's valuable data and information assets.

For any questions about data privacy, please contact any member of the Data Protection, Privacy, and Cybersecurity Team.

[1] These include (but certainly are not limited to): the Children's Online Privacy Protection Act (15 U.S.C. § 6501), the Telephone Consumer Protection Act (47 U.S.C. § 227), the Gramm Leach Bliley Act (15 U.S.C. §§ 6802(a), *et seq*.), the Fair and Accurate Credit Transactions Act (15 U.S.C. § 1681), the Family Educational Rights and Privacy Act (20 U.S.C. § 1232g), and the Health Information Portability and Accountability Act (29 U.S.C. §§ 1181, *et seq*.).