

Data Privacy Regulations

Small-business owners need privacy policies that promotes innovation and economic growth, with responsible, transparent use of data

Problem:

Governments both domestically and internationally are enacting internet privacy rules that could prove complex and burdensome for many unsuspecting small businesses. On May 25, 2018, the General Data Protection Regulation (GDPR) went into effect as passed by the European Union to strengthen and harmonize European data privacy laws and empower EU citizens' ability to control the use of their personal data. Efforts to mimic this law are underway in the U.S. - in 2018, California enacted a similar law which will be effective in 2020

- The GDPR requires: all personal data collected online to be securely encrypted; data breaches must be disclosed to all affected within 72 hours; and websites to disclose data collection and describe what data is going to be stored, how it is going to be used, and provide an opt-out.
- Regardless of its size and geographic reach, if a business sells good or provides services to either influence or monitor EU citizens, the GDPR applies. Thus, any company with a digital presence that collects, processes, manages or stores the data of European citizens will have to comply with the law or face steep penalties.
- Several U.S. states have recently introduced and passed legislation to expand data breach notification rules that mirror some of the protections provided by Europe's newly enacted GDPR.
- Like their European counterparts, these state laws are intended to provide consumers with greater transparency and control over their personal data, but go beyond breach notification and require companies to make significant changes in their data processing operations.
- The California Consumer Privacy Act, is enforceable in California and applies to California users, but given the nature of data processing, most companies will need to consider whether to apply the rules to all users.
- While these state laws give consumers unprecedented control over their personal information, it creates new and onerous challenges for companies of all sizes that do business in California.
- With GDPR and the new California law, managing personal data and keeping it secure will continue to get more expensive for business owners, forcing businesses to look for other technological solutions to help ease their compliance burden and manage risk when they engage in buying and selling of personal data.
- For now, it appears companies that restructured their operations to comply with GDPR will have to expand their efforts for California, and given the likelihood that other states will follow suit, there is likely to be a wave of GDPR-like activity in the U.S. ahead of California's 2020 deadline.
- As of March 2018, all 50 U.S. states, as well as the District of Columbia, Guam, Puerto Rico and the U.S. Virgin Islands, have enacted breach notification laws that require businesses to notify consumers if their personal information is compromised. These new and amended state data breach laws expand the definition of personal information and specifically mandate that certain information security requirements are implemented.

Solution:

While the GDPR may offer many important personal protections and rights that can be adapted in the U.S. - including greater transparency and data access rights - NSBA believes we need a robust law that fits our legal system, one that targets abuses, encourages innovation, and permits reasonable flexibility.

- While Congress had not yet enacted a comprehensive national privacy law, it does have a long history of passing privacy laws to protect some of the most sensitive types of personal data, such as financial and medical information and data concerning children.
- Before the recent election, scores of bipartisan bicameral privacy bills were introduced indicating a Congressional drive to address this issue. Any such legislation must consider the burden on small business—direct and indirect—and take steps to avoid stymieing innovation and competitiveness.

Learn More:

- [Click here to download NSBA's Economic Report Special Section on Cybersecurity](#)