Foster Garvey

# Happy Data Privacy Day – What Are You Doing to Keep Your Data Secure?

Legal Alert
January 28, 2022
*Foster Garvey Newsroom*

**Related Services**

Commercial & IP Transactions

IP & Technology

Privacy, Cybersecurity & Data Protection

Data Privacy Day is celebrated on January 28 each year to raise awareness about the importance of respecting privacy, safeguarding data and enabling trust. In honor of Data Privacy Day, now is an ideal time to review your company's privacy hygiene. Just like a regular visit to your doctor or dentist, privacy hygiene requires a periodic check-up.

Here are five quick but important tips you can use to minimize your risk:

- **Conduct a security assessment.** You can't have privacy without security. *Have you checked that your patch management process is working? Are you using multifactor authentication? When is the last time you took an inventory assessment?* While every business should develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of personal information, how those goals are accomplished depends on the type(s) of personally identifiable information it is collecting, how it is using the information and what is appropriate for the size and complexity of the business.

- **Create engaging employee training.** Help your employees understand the importance of data privacy. Currently, people are the biggest cybersecurity risk. While it is important to have technical controls, those controls can become meaningless if an employee falls prey to a phishing scam. Educate employees on the importance of privacy in their home and work lives, and then test the effectiveness of the training.

- **Review your privacy policy.** Check that your privacy policy is consistent with your current data collection and use practices. (*Do you know what your current data collection and use practices are?* If not, start there.) Ensure that you have updated your privacy policy to comply with the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR), as needed.

- **Build privacy into your business.** There are many possible privacy frameworks to help you build privacy measures into your business. Check out NIST, ISO, privacy by design and Fair Information Practice Principles to start. The most important factor is to figure out what works for your business. There is no "one size fits all" approach for determining appropriate privacy controls.

- **Implement an incident response plan.** If you don't already have an incident response plan (IRP), now's the best time to designate a point person to determine how to prepare, detect, contain, eradicate, recover and analyze. If you've been lucky enough to elude a data security incident, it's a matter of when, not if. Having an incident response plan helps your business timely respond to an incident and reduce both out-of-pocket costs and reputational damage. If you do have an incident response plan, *when's the last time you reviewed, tested and updated it?*

If you need assistance reviewing your company's compliance with privacy obligations, please contact our Privacy, Cybersecurity & Data Protection team.