WARD AND SMITH, P.A.
ATTORNEYS AT LAW

Data Privacy Part 1: The New Currency Businesses Should Protect and Here's How

Written By **Angela P. Doughty, CIPP/US** (apd@wardandsmith.com)
April 1, 2022

This is Part 1 of 2 in a series.

Data is king in today's digital economy. The estimated net worth of this global data market is forecast to hit nearly $235 billion by 2026, meaning collecting and sharing personal information is big business.

But with various regulations affecting how companies collect, store, and share data, including the California Privacy Act and EU's General Data Protection Regulation, and more consumers being concerned about how their data is used, data privacy is quickly becoming good for business.

For companies to safely take advantage of this marketing tool, here are some things you should know about data privacy to help your organization handle data the right way.

What is Personal Data?

The answer: it depends.

The definition of personal data can vary from state to state and country to country, making this a potential compliance nightmare. Complicating matters is the public's perception of what also constitutes personal information, regardless of any legal definitions.

This can put businesses in a no-win situation. On the one hand, violating regulations can cause costly fines and hit to a company's reputation. On the other, even if the leaked information wasn't classified as protected information, it can still result in a company losing consumer business.

The Data Golden Rule

Respecting consumers' privacy is a smart strategy for inspiring trust and enhancing reputation and growth in your business.

Therefore, treat consumers' private information like you want your personal data to be treated. Be upfront about what information your organization collects and why, and only gather information pertinent to your

business.

Have a transparent and informative privacy policy posted on your website or mobile app, and keep it up to date.

Conduct Privacy Audits

Conducting routine privacy assessments and audits are a good way of identifying deficits in your data privacy policy. Researching and adopting a privacy framework can also help you manage risk and create a culture of privacy in your organization by building privacy into your business.

There are many different frameworks and some may work better than others depending on the company. These resources can help organizations get a sense of how to get started: NIST Privacy Framework, AICPA Privacy Management Framework, ISO/IEC 27701 - International Standard for Privacy Information Management.

Managing Third-Party Data Sharing

Notable data breaches, such as the cyberattacks on SolarWinds, Microsoft Exchange, and Accellion, have shown that vendor and other third-party breaches can affect your company as if it was the one directly attacked.

The same way you review your privacy policy, you should also conduct a thorough review of your third-party vendor. Companies need to have a rigorous checklist to ensure that their partners are taking cybersecurity and data privacy as seriously as your business.

Here are a few questions you should ask to get started:

- Does your company have written business continuity/disaster recovery plans? Are these plans tested periodically?
- Does your company hire an external audit firm to perform a compliance review of your operational controls?
- Does your company have a pre-employment screening policy for employees and contractors?
- Are files and records reviewed, retained, and purged according to legal requirements, contractual obligations, and service level agreements?

Make Data Privacy Everyone's Job

From opening phishing emails to leaving company computers unsecured, employees can often be the chink in your company's data privacy armor. Training your employees to be stewardesses of personal information is your first line of defense against external threats. It also creates a work culture that prioritizes privacy within their organization.

Look to educate employees on your company’s privacy policy and teach new employees about their role in your privacy culture during the onboarding process.

Businesses can also build on fundamentals by setting up ongoing training and awareness sessions, establishing fireside chats with leadership around cybersecurity, and building toolkits for employees to refer to daily.

Conclusion

Data privacy is one of the few things businesses can't afford to get wrong. Therefore, businesses must put their best foot forward regarding data privacy. These few steps can help them make significant strides in developing better privacy habits.

--