
*A publication of Pullman & Comley, LLC*

**Attorneys:**

- **Russell F. Anderson**
  randerson@pullcom.com
  203.330.2271
- **Timothy G. Ronan**
  tronan@pullcom.com
  203.674.7933
- **James T. Shearin**
  jtshearin@pullcom.com
  203.330.2240

# An Overview of Data Privacy and Protection Laws for Manufacturers

## September 24, 2021

by Russell F. Anderson

For many manufacturers, data privacy and protection laws may seem like legal concerns that apply to other, more consumer-facing companies. While that may be largely true, given the ubiquitous nature of data, no business can truly escape considering how data privacy and protection laws may apply to them.

Data Breach Notification Laws

Data breach notification laws require businesses to notify affected individuals as well as the State Attorney General's Office and in certain instances, the media, when unencrypted sensitive data may have been accessed by unauthorized persons. For example, in Connecticut's data breach notification law, sensitive data includes Social Security numbers, drivers' license numbers, credit card numbers or financial account information in combination with any required security code or password. In addition, to providing the required notices, Connecticut also requires that the business provide the affected individuals 2 years' worth of credit monitoring services. As a result, a recent IBM Security Study found that the average cost for data breach response per record lost was $150.

Even if your business is strictly B2B, sensitive data can be squirreled away in various and surprising ways in your systems. Your business likely has the Social Security numbers of your employees for tax reporting. Does your business ever collect Social Security numbers in connection with credit checks? Does your business collect passport information in connection with taking your best customers on a retreat?

Before a ransomware hacker compromises your systems, you should inventory where sensitive data exists and encrypt data that you need to keep and eliminate anything that is extraneous. If you have not purchased a cyberliability policy, this

may be a good time to consider doing so.

Data Protection Laws

If your organization or sales efforts are international in scope, baseline data protection laws, such as the European Union's General Data Protection Regulation (or GDPR) are unavoidable. These laws require businesses to not only post a privacy policy, but also to justify the reasons for collection of any personal data (not just sensitive information) and provide the "data subject" numerous rights regarding the use, retention and disclosure of his/her information. In addition, data transfers between entities (such as between a customer and its vendors) and between countries (especially transfers to the U.S.) must be properly documented. Fines for violation of the GDPR can be as high as 4% of global revenue.

While the United States does not yet have a similar federal privacy law to the GDPR, numerous states have started to adopt their own versions of a "baseline" privacy law. These states currently include California, Virginia and Colorado. Connecticut almost passed its own GDPR-like law at the close of the last legislative session in June.

We would be happy to assist your manufacturing business determine the extent to which these state and international laws apply to you and to assist in your compliance efforts.