Ohio Data Protection Act (Senate Bill 220)

What is the Data Protection Act?

The Data Protection Act went into effect on November 2, 2018. It provides an ***incentive*** to Government and Businesses, particularly small government agencies and small businesses, to ***implement*** an Industry Security Standard through voluntary action.

Organizations taking reasonable cybersecurity precautions that meet certain industry-recognized frameworks will now be afforded a "safe harbor" against tort claims alleging that a failure to implement reasonable cybersecurity measures resulted in a data breach concerning personal or restricted information.

Safe Harbor

In order to trigger this safe harbor, an entity must adopt cybersecurity measures designed to: (1) protect the security and confidentiality of personal information; (2) protect against any anticipated threats or hazards to the security or integrity of the personal information; and (3) protect against unauthorized access to and acquisition of information that is likely to result in a material risk of identity theft or other fraud.

The scale of the cybersecurity program should be based on the organization's size and complexity, the nature and scope of its activities, the sensitivity of the personal information protected under the program, the cost and availability of tools to improve its information security, and the resources available to the organization. The entity's cybersecurity measures must also "reasonably conform" to one of the industry-recognized frameworks listed in R.C. 1354.03. These frameworks include:

- National Institute of Standards and Technology's (NIST) Cybersecurity Framework (800-171, 800-53 and 800-53a)
- ISO 27000 family - Information Security Management
- Safeguards Rule, Title V, of the Gramm Leach Biley Act (GLB)
- Security Requirements of the HIPAA
- PCI Data Security Standard

What Can Ohio Companies Do to Take Advantage of the Data Protection Act?

This new defense provides Ohio businesses the opportunity to evaluate the personal information they create, receive, maintain, and transmit, as well as the program they have in place to protect that information. Businesses should first consult their latest data-mapping and system inventories to understand how information is flowing through the organization and then decide how it should be secured.

- *Perform a series of non-technical components and evaluation*
- *Complete several technical checks and modifications*
- *Training Program for Employees*
- *Develop an overall CyberSecurity Plan*
- *Follow-up with any updates or revisions to your selected Security Framework*

Have more questions about the Data Protection Act?

Contact us today to speak with one of our compliance experts
(614) 600-3999 or mtesta@ccssmart.com

Organizations that have made the switch to CCS

FARMERS INSURANCE usbank CBRE CB RICHARD ELLIS JPMorganChase