

# Summary of House Bill 180: Delaware's Data Breach Law

## What You Need to Know

On August 24, 2017, Governor John Carney signed into law the first update to Delaware's data breach law in more than a decade. The law enacts new requirements for Delaware's businesses for protecting personal information.

### When did the law go into effect?

April 14, 2018

### What is the requirement?

If you conduct business in Delaware and own, license or maintain personal information on Delaware residents, you are required to "implement and maintain reasonable procedures and practices to prevent the unauthorized acquisition, use, modification, disclosure, or destruction of personal information collected or maintained in the regular course of business."

### If the data I own, license or maintain is hacked, what is my obligation?

You must provide notice to affected individuals "without unreasonable delay, but not later than 60 days" unless you can determine after an appropriate investigation that the breach is "unlikely to result in harm." If the data breach includes Social Security numbers, you must offer Delaware residents credit monitoring services at no cost to them for a period of one year. If the affected number of Delaware residents exceeds 500, you must also notify the Delaware Attorney General.

### What does the actual notice need to look like?

Delaware law does not require a specific form of notice to let Delaware residents know that there has been a breach of security involving their personal information, but the Consumer Protection Unit at the Delaware Department of Justice has issued a Model Data Security Breach Notification Form to provide guidance if you must give such notice to Delaware residents, as well as a separate form to use when you must also provide notice to the Delaware Attorney General. The forms are available on the Attorney General's Data Security Breach webpage:

<https://attorneygeneral.delaware.gov/fraud/cpu/securitybreachnotification/>

### What about vendors?

Once it has been determined there has been a breach of security, a vendor must give immediate notice to the owner or licensee of the information without consideration of whether there is a risk of harm. This law assigns responsibility for the risk of harm analysis with the person that owns or licenses the information.

## What Counts as Personal Information?

The categories listed below must be associated with a Delaware resident's first name *or* initial and last name in combination with any of the categories below with the required password or security code

- Social Security number
- Driver's license number
- Financial account number
- Passport Number
- Username or email address in combination with a password or security question
- Medical information
- Health insurance information
- DNA profile
- Biometric data used to access information
- An individual taxpayer identification number

## What are some actionable steps I can take right now?

- **Encrypt** all sensitive data and store your encryption key in a safe place separate from the encrypted data (if encrypted data is breached, you don't have to provide notice unless the encryption key is also breached). **What is encryption?** Encryption is the process of converting sensitive information or data into an unrecognizable code to prevent unauthorized access. It is accessed with an encryption key.
- **Educate yourself and your staff** by attending a local cyber security training going on in the state. You can also take advantage of online resources:
  - Delaware SBDC DatAssured Program: <https://delawaresbdc.org/special-programs/data-assured/>
  - Delaware's DigiKnow page: <https://digiknow.dti.delaware.gov/>
  - CyberSecure My Business™: <https://staysafeonline.org/cybersecure-business/>
- **Build a relationship with a trusted security specialist.** Don't have one? The Delaware SBDC has a list of Delaware IT specialists.
- **Lock down your logins.** Use strong authentication (sometimes referred to as 2-factor or multifactor authentication) to restrict access to accounts and ensure only those with permission can access them. This also includes using and enforcing strong passphrases.
- **For more tips, visit:** <https://stopthinkconnect.org/tips-advice/general-tips-and-advice>

### Source:

- [Delaware Code, Title 6, Chapter 12B \(http://delcode.delaware.gov/title6/c012b\)](http://delcode.delaware.gov/title6/c012b).



*This article is for general information purposes, and is not intended to be and should not be taken as legal advice. If you have questions, please seek the guidance of a licensed attorney.*