DATA BREACH REQUIREMENTS AT•A•GLANCE

With cybersecurity making the headlines constantly, data breaches are at the forefront of everyone's mind. In order to protect consumers, states have taken matters into their own hands and have created laws which require companies to report breaches. It can become confusing if you do business in multiple states because you are required to abide by the laws of each state where you have consumers, even if you don't have a physical location there. We've compiled the different data breach requirements across the Southeast below.

For additional information on data breach requirements, contact one of our professionals at 205.769.3251 or visit www.warrenaverett.com.

Warren Averett
CPAs AND ADVISORS

STATE	ALABAMA	GEORGIA	FLORIDA	TENNESSEE	MISSISSIPPI
Breach Defined	Unauthorized acquisition of computerized data that includes covered info, excluding certain good faith acquisitions by employees or agents.	All businesses (including startup or smaller firms, corporate or noncorporate) seeking to minimize filings, paperwork and overall cost	All businesses with no common law employees	Unauthorized acquisition that materially compromises the security, confidentiality or integrity of the covered info, excluding certain good-faith acquisitions by employees or agents.Provides an effective tax tool and employee benefit with employer control. Roth contributions allowed for high income taxpayers.	All businesses except governmental agencies
Code in State Law	8-38-1 to 12	10-1-910 to 912	501.171	47-18-2107	75-24-29
Government Notification Required	Yes, if >1,000 residents notified	No	Yes, if > 499 residents notified	No	No
Deadline for Consumer Notice	No later than 45 days	Most expedient time possible without reasonable delay	No later than 30 days	No later than 45 days	Without reasonable delay
Breach Based on Harm Threshold	Yes	No	Yes	No	Yes
Reasonable Security Measures	X (3.a)		X (171.2)		
Person Identified to Coordinate Security Measures	X (3.b.1)				
Identification of Internal Risks	X (3.b.2)				
Adoption and Testing of the Effectiveness of Information Safeguards	X (3.b.3)	X (910-4)			
Ongoing Evaluation of Security Measures to Account for Changes	X (3.b.5)				
Periodic Assessment of the Entity's Security Measures as a Whole	X (3.c)				
Procedures to Ensure That a Breach by an Unauthorized User Is Easily Identifiable		X (910-5)			
Procedures to Dispose of Personal Information After the Use Period Has Ended			X (171.4.f.8)		