

Corbett White and Davis P.A.

ATTORNEYS AT LAW
1111 Hypoluxo Road, Suite 207

Lantana, Florida 33462

JOHN CORBETT
TRELA J. WHITE
KEITH W. DAVIS*
JENNIFER GARDNER ASHTON
ERIN L. DEADY, P.A., of Counsel**

TELEPHONE (561) 586-7116
TELECOPIER (561) 586-9611

* Board Certified in City, County and Local Government Law
**AICP, LEED AP


MEMORANDUM

TO: Richard Radcliffe,
Executive Director of the Palm Beach County League of Cities, Inc.

FROM: Trela J. White, Esq., General Counsel

DATE: August 11, 2014

RE: Florida Information Protection Act of 2014, Effective July 1, 2014



As an update for all our members, I offer the following re: the above referenced legislation.

1. The Florida Information Protection Act was passed by the State Legislature as Chapter 2014-189 and is codified at Section 501.171, F.S. Such legislation specifically repealed Section 817.5681, F.S. and moved parts of the repealed Section to cp. 501, F.S. This new law provides for an expanded version of the requirements found in Section 817.5681, F.S. and attempts to protect personal information stored in electronic data bases of "Covered Entities". Governmental entities are included in that definition; thus a brief outline of the history and required actions may prove useful to municipalities.

2. 817.5681 F.S. "Breach of Security concerning confidential personal information in third party possession; administrative penalties" was adopted in 2005, and states in pertinent part, as follows:

Any person who conducts business in Florida and maintains computerized data, in a system that includes personal information:

Shall provide notice of any breach of the security of the system, following a determination of the breach to any resident of this State whose unencrypted personal information was or is reasonably believed, to have been acquired by an unauthorized person.

3. The above-referenced Section of the law contained time frames for reporting breaches and penalties for failure to do so; and encompassed approximately two (2) pages of detailed requirements. This law has been on the books for nearly nine (9) years, but has now been transferred to Section 501.171, Florida Statutes and has been expanded significantly. It provides for definitions, requirements for data security, notice to the State Department of Legal Affairs for security breaches and the form of such notice, as well as notice to the affected individuals.

4. In essence, the new Section of the State Law was effective July 1, 2014 and required all Covered Entities as defined in the Statutes to report any “breach of security” affecting five hundred (500) or more Florida residents. Reporting must be made to the State Department of Legal Affairs within thirty (30) days of the discovery of a breach or the belief that a breach has occurred. Covered Entities must also notify individuals whose personal information has been or is reasonably believed to have been accessed as a result of the breach. Notice to individuals must be made as expeditiously as possible, but no later than thirty (30) days after the breach or suspected breach. This “notice to individuals” reporting requirement may be waived if the applicable federal, state or local law enforcement agency believes it would interfere with a criminal investigation, or if, after an appropriate investigation, the Covered Entity reasonably believes that the breach has not and will not likely result in identity theft or other financial harm to the individuals.

5. Business and governmental entities must take reasonable measures to protect data in electronic form such as encrypting data or “de-identifying” the data. They must also dispose of records in a way that protects consumer information such as shredding, deleting, erasing or otherwise making certain the information is unreadable or undecipherable.

6. Entities that store data from Covered Entities must notify the Covered Entity within ten (10) days after discovering a breach or suspected breach in order that the Covered Entity may comply with the reporting requirements noted above.

7. “Personal Information” is defined as being any of the following:

A. An individual’s first name or first initial and last name in combination with any one of more of the following data elements for that individual:

1. A social security number
2. A driver’s license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity;
3. A financial account number or credit card or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual’s financial account;
4. Any information regarding an individual’s medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or
5. An individual’s health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual.

B. A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account.

C. The term does not include information about an individual that has been made publicly available by a federal, state, or local governmental entity. The term also does not include information that is encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable.

8. Violations of this section of the State Statute are treated as unfair and deceptive trade practices. Additionally a Covered Entity that violates the reporting sections of the law shall be liable for a civil penalty not to exceed Five Hundred Thousand Dollars (\$500,00.00) calculated as follows:

A. One Thousand Dollars (\$1,000.00) for each day up to the first thirty (30) days following any reporting violation and thereafter fifty thousand dollars (\$50,000.00) for

each subsequent thirty (30) day period or portion thereof for up to one hundred eighty (180) days; and

B. If the violation continues for more than one hundred eighty (180) days, in an amount not to exceed five hundred thousand dollars (\$500,000.00).

9. This newly expanded Information Protection Law does not alter or modify the Public Records Act, but simply requires extreme care when storing personal information of individuals in an electronic database.

Should additional information be desired, please advise.