

HOUSE OF REPRESENTATIVES STAFF ANALYSIS

BILL #: HB 7047 PCB OTM 19-12 OGSR/Security Breach Information
SPONSOR(S): Oversight, Transparency & Public Management Subcommittee, Good
TIED BILLS: **IDEN./SIM. BILLS:** SB 7008

REFERENCE	ACTION	ANALYST	STAFF DIRECTOR or BUDGET/POLICY CHIEF
Orig. Comm.: Oversight, Transparency & Public Management Subcommittee	15 Y, 0 N	Harrington	Harrington
1) Civil Justice Subcommittee	15 Y, 0 N	Deatherage	Poche
2) State Affairs Committee			

SUMMARY ANALYSIS

The Open Government Sunset Review Act requires the Legislature to review each public record exemption and each public meeting exemption five years after enactment. If the Legislature does not reenact the exemption, it automatically repeals on October 2nd of the fifth year after enactment.

The Florida Information Protection Act requires certain private and governmental entities to take reasonable steps to secure electronically held personal information and to report larger security breaches that compromise this information. Specifically, such entities must notify:

- Affected individuals when the breach will likely result in identity theft or other financial harm to those individuals; and
- The Department of Legal Affairs (department) in the event of a breach of data security involving access to the personal information of at least 500 individuals in this state.

Current law provides a public record exemption for all information received by the department pursuant to a notification of a data breach or received by the department pursuant to an investigation of such breach until the investigation is completed or ceases to be active.

The bill reenacts the public record exemption, which will repeal on October 2, 2019, if this bill does not become law.

The bill does not appear to have a fiscal impact on the state or local governments.

FULL ANALYSIS

I. SUBSTANTIVE ANALYSIS

A. EFFECT OF PROPOSED CHANGES:

Background

Open Government Sunset Review Act

The Open Government Sunset Review Act¹ sets forth a legislative review process for newly created or substantially amended public record or public meeting exemptions. It requires an automatic repeal of the exemption on October 2nd of the fifth year after creation or substantial amendment, unless the Legislature reenacts the exemption.²

The Act provides that a public record or public meeting exemption may be created or maintained only if it serves an identifiable public purpose. In addition, it may be no broader than is necessary to meet one of the following purposes:

- Allow the state or its political subdivisions to effectively and efficiently administer a governmental program, which administration would be significantly impaired without the exemption.
- Protect sensitive personal information that, if released, would be defamatory or would jeopardize an individual's safety; however, only the identity of an individual may be exempted under this provision.
- Protect trade or business secrets.³

If, and only if, in reenacting an exemption that will repeal, the exemption is expanded (essentially creating a new exemption), then a public necessity statement and a two-thirds vote for passage are required.⁴ If the exemption is reenacted with grammatical or stylistic changes that do not expand the exemption, if the exemption is narrowed, or if an exception to the exemption is created⁵ then a public necessity statement and a two-thirds vote for passage are not required.

The Florida Information Protection Act of 2014

In 2014, the Legislature enacted the Florida Information Protection Act (act), which requires private and governmental "covered entities"⁶ to take reasonable steps to secure electronically held personal information and to report larger security breaches that compromise this information. Specifically, covered entities must notify:

- Affected individuals when the breach will likely result in identity theft or other financial harm to those individuals; and
- The Department of Legal Affairs (department) in the event of a breach of data security involving access to the personal information of at least 500 individuals in this state.⁷

Such notice must be provided to the department as expeditiously as practicable, but no later than 30 days after the determination of the breach.⁸

¹ Section 119.15, F.S.

² Section 119.15(3), F.S.

³ Section 119.15(6)(b), F.S.

⁴ Section 24(c), Art. I of the State Constitution.

⁵ An example of an exception to a public record exemption would be allowing another agency access to confidential and exempt records.

⁶ Section 501.171(1)(b), F.S., defines the term "covered entities" to mean a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity that acquires, maintains, stores, or uses personal information. For purposes of the reporting requirements, the term includes governmental entities.

⁷ Section 501.171(3)(a), F.S.

⁸ *Id.*

A breach of security is defined as an unauthorized access of data in electronic form containing personal information. The term “personal information” includes a person’s name along with:⁹

- A social security number;
- A driver license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity;
- A financial account number or credit or debit card number in combination with a required security or access code or password necessary to gain access to the person’s financial account;
- Certain medical information; or
- A person’s health insurance policy number or subscriber identification number or similar identifier.

The term “personal information” also includes a username or e-mail address in combination with a password or security question and answer that permits access to an online account.¹⁰

Public Record Exemption under Review

In 2014, the Legislature created a public record exemption for all information received by the department pursuant to a notification of a data breach or received by the department pursuant to a data breach investigation until such time as the investigation is completed or ceases to be active.¹¹ Such information is confidential and exempt¹² from s. 119.07(1), F.S., and s. 24(a), Art. I of the State Constitution.¹³

During the investigation, confidential and exempt information may be disclosed by the department:

- In the furtherance of its official duties and responsibilities;¹⁴
- For print, publication, or broadcast if the department determines that such release would assist in notifying the public or locating or identifying a person that the department believes to be a victim of a data breach or improper disposal of customer records, except for information that remains confidential and exempt even after the investigation is completed; and
- To another governmental entity in the furtherance of its official duties and responsibilities.

Upon completion of an investigation or once an investigation ceases to be active, the following information received by the department must remain confidential and exempt:¹⁵

- All information to which another public records exemption applies;
- Personal information;
- A computer forensic report;
- Information that would otherwise reveal weakness in a covered entity’s data security; and
- Information that would disclose a covered entity’s proprietary information.

⁹ Section 501.171(1)(g), F.S.

¹⁰ *Id.*

¹¹ Chapter 2014-190, L.O.F.; codified as s. 501.171(11), F.S.

¹² There is a difference between records the Legislature designates as exempt from public record requirements and those the Legislature deems confidential and exempt. A record classified as exempt from public disclosure may be disclosed under certain circumstances. *See WFTV, Inc. v. The School Board of Seminole*, 874 So.2d 48, 53 (Fla. 5th DCA 2004), review denied 892 So.2d 1015 (Fla. 2004); *City of Riviera Beach v. Barfield*, 642 So.2d 1135 (Fla. 4th DCA 1994); *Williams v. City of Minneola*, 575 So.2d 687 (Fla. 5th DCA 1991). If the Legislature designates a record as confidential and exempt from public disclosure, such record may not be released by the custodian of public records to anyone other than the persons or entities specifically designated in statute. *See* Attorney General Opinion 85-62 (August 1, 1985).

¹³ Section 501.171(11)(a), F.S.

¹⁴ Section 501.171(11)(b), F.S.

¹⁵ Section 501.171(11)(c), F.S.

The 2014 public necessity statement for the exemption provided in relevant part that:

A notification of a violation of s. 501.171, Florida Statutes, is likely to result in an investigation of such violation because a data breach is likely the result of criminal activity. The premature release of such information could frustrate or thwart the investigation and impair the ability of the [department] to effectively and efficiently administer [the act]. In addition, release of such information before completion of an active investigation could jeopardize the ongoing investigation . . . An investigation of a data breach or improper disposal of customer records is likely to result in the gathering of sensitive personal information, including social security numbers, identification numbers, and personal financial and health information. Such information could be used for the purpose of identity theft. In addition, release of such information could subject possible victims of the data breach or improper disposal of customer records to further financial harm . . . Release of a computer forensic report or other information that would otherwise reveal weakness in a covered entity's data security could compromise the future security of that entity, or other entities, if such information were available upon conclusion of an investigation or once an investigation ceases to be active.¹⁶

Pursuant to the Open Government Sunset Review Act, the exemption will repeal on October 2, 2019, unless reenacted by the Legislature.¹⁷

During the 2018 interim, subcommittee staff sent a questionnaire to the department regarding the department's use of the public record exemption. According to the department, the exemption has provided protection to the confidential and exempt information during the course of the investigation, allowing the department to properly investigate security breaches. In addition, the department believes that disclosure of sensitive personal data could result in identity theft, financial harm, and disclosure of personal health matters. As such, the department recommends reenactment of the public record exemption.

Effect of the Bill

HB 7047 removes the scheduled repeal date of the public record exemption, thereby reenacting the public record exemption for all information received by the department pursuant to a notification of a data breach or received by the department pursuant to a data breach investigation until such time as the investigation is completed or ceases to be active.

B. SECTION DIRECTORY:

Section 1: Amends s. 501.171, F.S., to save from repeal the public record exemption for all information received by the department pursuant to a notification of a data breach or received by the department pursuant to an investigation of a data breach.

Section 2: Provides an effective date of October 1, 2019.

¹⁶ Section 2, ch. 2014-190, L.O.F.

¹⁷ Section 501.171(11)(e), F.S.

II. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT

A. FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues:

None.

2. Expenditures:

None.

B. FISCAL IMPACT ON LOCAL GOVERNMENTS:

1. Revenues:

None.

2. Expenditures:

None.

C. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR:

None.

D. FISCAL COMMENTS:

None.

III. COMMENTS

A. CONSTITUTIONAL ISSUES:

1. Applicability of Municipality/County Mandates Provision:

Not applicable. This bill does not appear to affect county or municipal governments.

2. Other:

None.

B. RULE-MAKING AUTHORITY:

None.

C. DRAFTING ISSUES OR OTHER COMMENTS:

None.

IV. AMENDMENTS/ COMMITTEE SUBSTITUTE CHANGES