

Commerce Committee

Thursday, February 10, 2022
9:00 AM - 11:00 AM
Webster Hall (212 Knott)

Meeting Packet

Chris Sprowls
Speaker

Blaise Ingoglia
Chair

The Florida House of Representatives

Commerce Committee

Chris Sprowls
Speaker

Blaise Ingoglia
Chair

Meeting Agenda

Thursday, February 10, 2022
9:00 AM – 11:00 AM
Webster Hall (212 Knott)

I. Call to Order

II. Roll Call

III. Welcome and Opening Remarks

IV. Consideration of the following bill(s):

- HB 9 Consumer Data Privacy by McFarland
- HB 631 Airport Funding by Grall
- HB 695 Property Insurer Reimbursements by Stevenson
- HB 1565 Pub. Rec./Consumer Data Privacy by McFarland

V. Closing Remarks

VI. Adjournment

303 House Office Building, 402 South Monroe Street, Tallahassee, FL 32399-1300
(850) 717-4870

HB 9

HOUSE OF REPRESENTATIVES STAFF ANALYSIS

BILL #: HB 9 Consumer Data Privacy
SPONSOR(S): McFarland
TIED BILLS: HB 1565 **IDEN./SIM. BILLS:**

REFERENCE	ACTION	ANALYST	STAFF DIRECTOR or BUDGET/POLICY CHIEF
1) Commerce Committee		Wright	Hamon
2) Judiciary Committee			

SUMMARY ANALYSIS

Due to the growth in businesses that collect personal information for the purpose of selling targeted advertising on the Internet, many countries and states have adopted or updated laws relating to the collection and use of personal information. Specifically, the European Union, and states like California, Virginia, Colorado, and Illinois, have enacted data privacy laws to protect consumers' personal information.

The bill requires certain businesses to publish a privacy policy for personal information, and defines "personal information" as information that is linked or reasonably linkable to an identified or identifiable consumer or household, including biometric information and unique identifiers to the consumer. The term does not include certain public information, certain employee information, or deidentified or aggregate information.

The bill gives consumers rights related to personal information collected by certain businesses, including:

- The right to access personal information collected,
- The right to delete or correct personal information, and
- The right to opt-out of the sale or sharing of personal information.

The bill allows the Department of Legal Affairs (DLA) to enforce these rights by bringing an action against, and collecting civil penalties from, violators. Consumers whose personal information has been sold or shared after opting-out, or has been retained after a request to delete or correct may also bring a cause of action.

The bill also adds "biometric data" to the definition of "personal information" in the Florida Information Protection Act. Thus, entities in possession of fingerprints, DNA, and other biological or physiological identifying information must take reasonable measures to protect the biometric data and report data breaches.

The bill has no fiscal impact on local governments, and an indeterminate fiscal impact on state government.

The bill has an effective date of July 1, 2023.

FULL ANALYSIS

I. SUBSTANTIVE ANALYSIS

A. EFFECT OF PROPOSED CHANGES:

Consumer Data Privacy – Current Situation

Florida Deceptive and Unfair Trade Practices Act (FDUTPA)

FDUTPA is a consumer and business protection measure that prohibits unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in trade or commerce.[1] FDUTPA is based on federal law.[2]

DLA or the Office of the State Attorney (SAO) may bring actions when it is in the public interest on behalf of consumers or governmental entities.[3] SAO may enforce violations of the FDUTPA if the violations take place in its jurisdiction. DLA has enforcement authority if the violation is multi-jurisdictional, the state attorney defers in writing, or the state attorney fails to act within 90 days after a written complaint is filed.[4] In certain circumstances, consumers may also file suit through private actions.[5]

DLA and the SAO have powers to investigate FDUTPA claims, which include:[6]

- Administering oaths and affirmations,
- Subpoenaing witnesses or matter, and
- Collecting evidence.

DLA and the State Attorney, as enforcing authorities, may seek the following remedies:

- Declaratory judgments,
- Injunctive relief,
- Actual damages on behalf of consumers and businesses,
- Cease and desist orders, and
- Civil penalties of up to $10,000 per willful violation.[7]

FDUTPA may not be applied to certain entities in certain circumstances, including:[8]

- Any person or activity regulated under laws administered by the Office of Insurance Regulation or the Department of Financial Services; or
- Banks, credit unions, and savings and loan associations regulated by the Office of Financial Regulation or federal agencies.

Consumer Data

[1] Ch. 73-124, L.O.F., and s. 501.202, F.S.
[2] D. Matthew Allen, et. al., *The Federal Character of Florida's Deceptive and Unfair Trade Practices Act*, 65 U. MIAMI L. REV. 1083 (Summer 2011).
[3] S. 501.207(1)(c) and (2), F.S.; *see* s. 501.203(2), F.S. (defining "enforcing authority" and referring to the office of the state attorney if a violation occurs in or affects the judicial circuit under the office's jurisdiction; or the Department of Legal Affairs if the violation occurs in more than one circuit; or if the office of the state attorney defers to the department in writing; or fails to act within a specified period.); *see also* David J. Federbush, *FDUTPA for Civil Antitrust: Additional Conduct, Party, and Geographic Coverage; State Actions for Consumer Restitution*, 76 FLORIDA BAR JOURNAL 52, Dec. 2002 (analyzing the merits of FDUPTA and the potential for deterrence of anticompetitive conduct in Florida), *available at* http://www.floridabar.org/divcom/jn/jnjournal01.nsf/c0d731e03de9828d852574580042ae7a/99aa165b7d8ac8a485256c8300791ec1!OpenDocument&Highlight=0,business,Division* (last visited on Jan. 28, 2022).
[4] S. 501.203(2), F.S.
[5] S. 501.211, F.S.
[6] S. 501.206(1), F.S.
[7] Ss. 501.207(1), 501.208, and 501.2075, F.S. Civil Penalties are deposited into general revenue. Enforcing authorities may also request attorney fees and costs of investigation or litigation. S. 501.2105, F.S.
[8] S. 501.212(4), F.S.

As technologies that capture and analyze data proliferate, so, too, do businesses' abilities to contextualize consumer data. Businesses use it for a range of purposes, including better understanding of day-to-day operations, making more informed business decisions and learning about their customers.[9]

From consumer behavior to predictive analytics, companies regularly capture, store, and analyze large amounts of quantitative and qualitative data on their consumer base. Some companies have built an entire business model around consumer data, whether the companies are selling personal information to a third party or creating targeted ads.[10]

Generally, the types of consumer data that businesses collect are:[11]

- Personal data, which includes personally identifiable information, such as Social Security numbers and gender, as well as identifiable information, including IP address, web browser cookies, and device IDs;
- Engagement data, which details how consumers interact with a business's website, mobile apps, social media pages, emails, paid ads and customer service routes;
- Behavioral data, which includes transactional details such as purchase histories, product usage information, and qualitative data; and
- Attitudinal data. This data type encompasses metrics on consumer satisfaction, purchase criteria, product desirability and more.

[9] Max Freedman, How Businesses Are Collecting Data (And What They're Doing With It), Business News Daily (Jun. 17, 2020) https://www.businessnewsdaily.com/10625-businesses-collecting-data.html (last visited Jan. 28, 2022).
[10] *Id.*
[11] *Id.*

Comparison of Consumer Data Privacy Laws [12]

Comparison of Consumer Data Privacy Laws				
Element	**Colorado**	**Virginia**	**California**	**European Union**
Opt-out or Opt-in of Sale of Personal Information	Opt-Out	Opt-Out	Opt-Out	Opt-In
Opt-in or Opt-out of Sensitive Information Processing	Opt-In	Opt-In	Opt-Out	Opt-In
Statutory Cure Period	✓	✓	✓	X
Right to Appeal Denials or Requests	✓	✓	X	X
Express Obligations for Deidentified Data	✓	✓	X	X
Requirement to Perform Data Impact Assessments	✓	✓	✓	✓
Private Right of Action	X	X	✓	✓
Government Enforcement Agency	Attorney General	Attorney General	CPPA, Attorney General	DPAs
Penalties	Up to $20,000 per violation	Up to $7,500 per violation	Up to $2,500 per unintentional violation, and up to $7,500 per intentional violation	Up to €20 million, or 4% of worldwide annual revenue for violations, depending on severity of the violation
Operative Date	07/01/23	01/01/23	01/01/23	05/25/18
Business/Controller Applicability Thresholds	Either: •Controls/Processes data of at least 100,000 consumers per year; or •Derives revenue from sale of data from at least 25,000 consumers per year	Either: •Controls/Processes data of at least 100,000 consumers per year; or •Derives over 50% of revenue from sale of data from at least 25,000 consumers per year	Meets any of the following: •Gross annual revenue of over $25 million; •Processes data of 100,000 or more consumers; or •Derives at least 50% or more of revenue from data sales	•Any E.U. business which processes consumer data; or •Any worldwide business that offers goods/services (paid or for free) or is monitoring the behavior of individuals in the E.U.

General Data Protection Regulation (European Union)

In 2016, The European Union passed a broad data privacy law that addressed several areas of consumer rights and data protection called the General Data Protection Regulation (GDPR).[13] The law became effective in 2018 and unified the regulatory approach to data privacy across the European Union. The GDPR has since become a model for other data privacy laws in other countries, including Chile, Japan, Brazil, South Korea, Argentina, and Kenya.[14]

Under the GDPR, personal data is anything that allows a person to be identified. Under GDPR, individuals, organizations, and companies that are either 'controllers' or 'processors' of personal data

[12] JDSupra, *Virginia Is For Lovers…Of Data Privacy*, https://www.jdsupra.com/legalnews/virginia-is-for-lovers-of-data-privacy-3879845/ (last visited Jan. 28, 2022).
[13] European Data Protection Supervisor, The History of the General Data Protection Regulation, https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en (last visited Jan. 28, 2022).
[14] *Id.*

are covered by the law. Controllers exercise overall control over the purposes and means of processing personal data. Processors act on behalf of, and only on the instructions of, the relevant controller.[15]

Before processing or collecting any personal data, any business must ask for explicit permission from the subject or person. The request must use clear language. **This is known as an "opt-in."**

The provisions of the GDPR specifically ban the use of long documents filled with legalese - hiding permissions within Terms and Conditions or a Privacy Policy will not meet the requirements. **Consent** must be given for a specific purpose and must be requested separately from other documents and policy statements.[16]

The GDPR requires companies to provide, at the data subject's request, confirmation as to whether personal data pertaining to them is being processed, where it is being processed, and for what purpose. Companies must also be able to provide, free of charge**, a copy of the personal data** being processed in an electronic format.[17]

Under the GDPR, companies must erase all personal data when asked to do so by the data subject. At that point, the company must cease further dissemination of the data, and halt all processing. Valid conditions for erasure include situations where the data is no longer relevant, or the original purpose has been satisfied, or merely a data subject's subsequent withdrawal of consent.[18]

The GDPR requires companies to provide mechanisms for a data subject to receive any previously provided personal data in a commonly used and machine-readable format.[19]

The GDPR allows private rights of action for violations of privacy rights, but the consumer must prove any damages in order to receive compensation.[20]

California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA)

The California Consumer Privacy Act of 2018 (CCPA) was passed to give consumers more control over the personal information that businesses collect. This landmark law in the United States granted new **privacy rights** for California consumers, including:[21]

- The right to know about the personal information a business collects, specifically about the consumer, and how it is used and shared;
- The right to delete personal information collected with some exceptions;
- The right to **opt-out** of the sale of personal information; and
- The right to non-discrimination for exercising the CCPA rights.

The CCPA applies to for-profit businesses that do business in California that also meet any of the following:[22]

- Have a gross annual revenue of over $25 million;
- Buy, receive, or sell the personal information of 50,000 or more California residents, households, or devices; or
- Derive 50 percent or more of their annual revenue from selling California residents' personal information.

---

[15] Wired, What is the GDPR? The summary guide to GDPR compliance in the UK, https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018 (last visited Jan. 28, 2022).
[16] TechRepublic, GDPR: A cheat sheet, https://www.techrepublic.com/article/the-eu-general-data-protection-regulation-gdpr-the-smart-persons-guide/ (last visited Jan. 28, 2022).
[17] *Id*.
[18] *Id*.
[19] *Id*.
[20] Art. 82 of the GDPR.
[21] State of California Department of Justice, Office of the Attorney General, California Consumer Privacy Act (CCPA), https://oag.ca.gov/privacy/ccpa (last visited Jan. 28, 2022).
[22] Cal. Civ. Code § 1798.140.

Businesses are required to give consumers certain notices explaining their privacy practices and provide certain mechanisms to allow consumers to exercise their rights.[23]

The law is largely enforced by the Attorney General, and businesses are subject to fines for violating the law. Consumers may only bring a **cause of action** against a business if certain categories of personal information tied to their name have been stolen in a nonencrypted and nonredacted form.[24] As of July 2020, approximately 50 suits had been filed pursuant to this provision.[25]

The California Privacy Rights Act (CPRA) passed in 2020 as a statewide proposition, though it is not effective until **January 1, 2023**. The CPRA amends and expands the CCPA. Specifically dealing with certain areas of concern with the CCPA and it also created a new agency to handle complaints and enforcement. **The CPRA changes the CCPA** in the following ways:[26]

- Allowing consumers to:
  - prevent businesses from **sharing** personal information;
  - correct inaccurate personal information; and
  - limit businesses' use of "sensitive personal information"—including precise geolocation; race; ethnicity; religion; genetic data; private communications; sexual orientation; and specified health information;
- Establishing California Privacy Protection Agency to additionally enforce and implement consumer privacy laws and impose fines;
- Changing criteria for which businesses must comply with laws by:
  - Doubling the CCPA's threshold number of consumers or households **from 50,000 to 100,000**, resulting in reduced applicability of the law to small and midsize businesses;
  - Expanding applicability to businesses that generate most of their revenue from **sharing personal information, not just selling it**; and
  - Extending the definition to joint ventures or partnerships composed of businesses that each have at least a 40 percent interest.
- Prohibiting businesses' retention of personal information for longer than reasonably necessary;
- Tripling maximum penalties for violations concerning consumers **under age 16**; and
- Authorizing civil penalties for theft of consumer login information.

Virginia Consumer Data Protection Act

On March 2, 2021, the Virginia Consumer Data Protection Act (VCDPA) was signed into law.[27] The VCDPA, which will not become effective until **January 1, 2023**, borrows from CCPA and GDPR.[28] Some argue that because Virginia was able to benefit from the experience of businesses that have spent the better part of the last five years implementing GDPR or CCPA, the Virginia law may be a lighter implementation task for companies.[29]

Generally, with regard to personal data, the VCDPA grants consumers the **right to**:

- Access,
- Correct,
- Delete,
- Obtain a copy of, and
- Opt-out of the processing of personal data for the purposes of targeted advertising.

---

[23] Cal. Civ. Code §§ 1798.130, 1798.135.
[24] Cal. Civ. Code §§ 1798.150, 1798.155.
[25] Holland & Knight LLP, Litigating the CCPA in Court, https://www.hklaw.com/en/insights/publications/2020/07/litigating-the-ccpa-in-court (last visited Jan. 28, 2022).
[26] Ballotpedia, *California Proposition 24, Consumer Personal Information Law and Agency Initiative (2020)*, https://ballotpedia.org/California_Proposition_24,_Consumer_Personal_Information_Law_and_Agency_Initiative_(2020) (last visited Jan. 28, 2022).
[27] JDSupra, *Virginia's Consumer Data Protection Act Has assed: What's in It?*, https://www.jdsupra.com/legalnews/virginia-s-consumer-data-protection-act-1577777/ (last visited Jan. 28, 2022).
[28] Sidley Austin LLP, East Coast Meet West Coast: Enter the Virginia Consumer Data Privacy Protection Act, https://www.sidley.com/en/insights/newsupdates/2021/03/east-coast-meets-west-coast-enter-the-virginia-consumer-data-protection-act (last visited Jan. 28, 2022).
[29] *Id.*

VCDPA contains exceptions for certain types of data and information governed by federal law. It provides that the Attorney General has exclusive authority to **enforce violations** of the law, and does not provide a private cause of action to consumers. VCDPA applies to persons conducting business in the state that either:

- Control or process personal data of at least 100,000 consumers or
- Derive over 50 percent of gross revenue from the sale of personal data and control or process personal data of at least 25,000 consumers.[30]

Colorado Privacy Act

The Colorado Privacy Act (CPA)[31] was signed in to law on July 8, 2021, and is effective **July 1, 2023**. The law also borrows from the GDPR, CCPA, and VDCPA.[32]

Generally, with regard to personal data, the CPA grants consumers the **right to**:[33]

- Access,
- Correct,
- Delete, and
- Data portability.

Like the CCPA and VCDPA, CPA contains exceptions for certain types of data and information governed by federal law. It provides that the Attorney General has exclusive **authority to enforce** violations of the law, and does not provide a private cause of action to consumers. CPA applies to persons conducting business in the state that either:[34]

- Controls or processes personal data of 100,000 or more consumers during a calendar year; or
- Derive revenue or receive discounts from the sale of personal data and control or process data of at least 25,000 consumers.

Illinois Biometric Information Privacy Act

In 2008, Illinois adopted the Biometric Information Privacy Act (BIPA), which puts in place safeguards and procedures relating to the retention, collection, disclosure, and destruction of biometric information and specifically protects the biometric information of those in the state. It was the first state law in the U.S. to specifically regulate biometrics.

Under BIPA, a private entity:[35]

- In possession of biometric data (defined as retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry) must have a **written policy** establishing a retention schedule and guidelines for permanently destroying such data;
- May not collect, capture, purchase, receive through trade, or otherwise obtain biometric data unless it informs the subject that the data is being stored and the manner of storage, and receives a written release from the subject;
- May not profit from a person's biometric data;
- May not disseminate a person's biometric data **unless the subject consents**, is authorized by the subject, or is required by law or a valid warrant or subpoena; and
- Must store, transmit, and protect biometric data with a reasonable standard of care and in a manner as or more protective as other confidential and sensitive information.

[30] Virginia's Legislative Information System, Bill Summary for SB 1392, https://lis.virginia.gov/cgi-bin/legp604.exe?211+sum+SB1392S (last visited Jan. 28, 2022).
[31] C.R.S. 1-6-1301-1313
[32] The National Law Review, *And Now There are Three … The Colorado Privacy Act*, July 16, 2021, https://www.natlawreview.com/article/and-now-there-are-three-colorado-privacy-act#:~:text=Colorado%20has%20now%20joined%20California,effect%20on%20July%201%2C%202023. (last visited Jan. 27, 2022).
[33] *Id*.
[34] *Id*.
[35] 740 Ill. Comp. Stat. 14/10, 14/15 (2008).

BIPA provides a **private cause of action**, with relief including:[36]

- Liquidated damages of $1,000 or actual damages, whichever is greater, against a private entity that negligently violates BIPA;
- Liquidated damages of $5,000 or actual damages, whichever is greater, against a private entity that intentionally or recklessly violates BIPA;
- Reasonable attorneys' fees and costs; and
- Other relief, including an injunction, as the court deems appropriate.

Because Illinois granted a private cause of action for violations of BIPA, there have been several lawsuits claiming damages for privacy and use violations, and Illinois courts have upheld the law. On January 25, 2019, the Illinois Supreme Court found that an individual does not need to allege an actual injury or adverse effect, beyond violation of their rights under BIPA, to qualify as an aggrieved party. Therefore, anyone whose biometric data is affected by a violation of BIPA may seek liquidated damages or injunctive relief under the Act.[37] Court documents also tend to support the notion that an individual in Illinois has a valid cause of action if their biometric data is taken without consent by a private entity, including out-of-state entities, but it is subject to a finding of fact.[38]

Federal Laws Addressing Data Privacy

While there is no broad federal law addressing data privacy, generally, there are several industry-specific laws that address the need to keep certain data private or protected, including the following:

Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act of 1996 (HIPAA)[39] is a federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The U.S. Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule[40] to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.[41]

HIPAA's Privacy Rule protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "protected health information (PHI)" from being disclosed without the patient's consent or knowledge.[42]

"Individually identifiable health information" is information, including demographic data, that relates to:[43]

- The individual's past, present or future physical or mental health or condition,
- The provision of health care to the individual, or
- The past, present, or future payment for the provision of health care to the individual.

The Privacy Rule excludes from protected health information employment records that a covered entity maintains in its capacity as an employer and education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act.[44] 20 U.S.C. §1232g.

The Security Rule applies to the subset of identifiable health information a covered entity creates, receives, maintains, or transmits in electronic form, and is called "electronic protected health

[36] 740 Ill. Comp. Stat. 14/20 (2008).
[37] *Rosenbach v. Six Flags Entertainment Corporation*, 2019 IL 123186.
[38] *Rivera v. Google, Inc.*, 238 F.Supp.3d 1088 (N.D. Ill. 2017).; *In re Facebook Biometric Information Privacy Litigation*, 185 F.Supp.3d 1155 (N.D. Cal. (2016).; *Norberg v. Shutterfly, Inc.*, 152 F.Supp.3d 1103 (N.D. Ill. 2015).
[39] 42 U.S.C. § 1320.
[40] 45 C.F.R. §§ 160 and 164.
[41] Centers for Disease Control and Prevention, Health Insurance Portability and Accountability Act of 1996 (HIPAA), https://www.cdc.gov/phlp/publications/topic/hipaa.html (last visited Jan. 28, 2022).
[42] *Id*.
[43] 45 C.F.R. § 160.103.
[44] 20 U.S.C. § 1232(g).

information" (e-PHI). The Security Rule does not apply to PHI transmitted orally or in writing. To comply with the Security Rule, all covered entities must do the following:[45]

- Ensure the confidentiality, integrity, and availability of all electronic protected health information,
- Detect and safeguard against anticipated threats to the security of the information,
- Protect against anticipated impermissible uses or disclosures, and
- Certify compliance by their workforce.

"Covered entities" who must abide by the Privacy Rule and the Security Rule are:[46]

- Health plans,
- Healthcare providers,
- Healthcare clearinghouses, and
- Business associates.

Federal Policy for the Protection of Human Subjects

The Federal Policy for the Protection of Human Subjects, or the "Common Rule," is a rule promulgated by the U.S. Food and Drug Administration (FDA).[47] The Common Rule governs the ethical conduct of research involving human subjects. Fifteen federal agencies and departments are party to this rule, which first came into effect in 1981. The Common Rule has not been substantively updated since 1991.[48] Among other requirements, the Common Rule mandates that researchers protect the privacy of subjects and maintain confidentiality of human subject data.[49]

The FDA is a member of the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use, which brings together the regulatory authorities and pharmaceutical industry to develop guidelines for pharmaceutical trials.[50]

The Fair Credit Reporting Act

The Fair Credit Reporting Act[51] (FCRA) protects information collected by consumer reporting agencies such as credit bureaus, medical information companies and tenant screening services. Information in a consumer report cannot be provided to anyone who does not have a purpose specified in the FCRA. Companies that provide information to consumer reporting agencies also have specific legal obligations, including the duty to investigate disputed information. In addition, users of the information for credit, insurance, or employment purposes must notify the consumer when an adverse action is taken on the basis of such reports.[52]

The Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act[53] requires financial institutions, such as companies that offer consumers financial products or services like loans, financial or investment advice, mortgages, or insurance, to explain their information-sharing practices to their customers and to safeguard sensitive data.[54]

---

[45] CDC, supra note 40.
[46] 45 C.F.R. §§ 160.102, 160.103.
[47] 21 C.F.R. §§ 50, 60.
[48] Association of Public and Land-Grant Universities, The "Common Rule" Federal Policy for the Protection of Human Subjects, https://www.aplu.org/projects-and-initiatives/research-science-and-technology/common-rule/#:~:text=The%20Federal%20Policy%20for%20the,been%20substantively%20updated%20since%201991. (last visited Jan. 28, 2022).
[49] The University of Chicago, *University Data Usage Guide, Sensitive Identifiable Human Subject Research Data*, https://dataguide.uchicago.edu/sensitive-identifiable-human-subject-research-data (last visited Jan. 28, 2022).
[50] International Council for Harmonisation, Welcome to the ICH Official Website, https://www.ich.org/ (last visited Jan. 28, 2022).
[51] 15 U.S.C. § 1681.
[52] The Federal Trade Commission, Fair Credit Reporting Act, https://www.ftc.gov/enforcement/statutes/fair-credit-reporting-act (last visited Jan. 28, 2022).
[53] 15 U.S.C. § 6801.
[54] The Federal Trade Commission, Gramm-Leach-Bliley Act, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act (last visited Jan. 28, 2022).

The law requires that financial institutions protect information collected about individuals; it does not apply to information collected in business or commercial activities.

In certain situations, consumers of a financial institution have opt-out rights from having their nonpublic personal information shared with third parties.[55]

Driver's Privacy Protection Act

The Driver's Privacy Protection Act of 1994 (DPPA)[56] protects the privacy of personal information assembled by state departments of motor vehicles (DMVs).

The DPPA prohibits the release or use by any state DMV (or any officer, employee, or contractor thereof) of personal information about an individual obtained by the DMV in connection with a motor vehicle record, subject to certain exceptions, such as for legitimate government needs. It sets penalties for violations and makes violators liable on a civil action to the individual to whom the released information pertains.[57]

DPPA also requires states to get permission from individuals before their personal motor vehicle record may be sold or released to third-party marketers.[58]

Family Educational Rights and Privacy Act

The Family Educational Rights and Privacy Act (FERPA)[59] protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when they reach the age of 18 or attend a school beyond the high school level.

Schools may disclose, without consent, "directory" information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. However, schools must tell parents and eligible students about directory information and allow parents and eligible students a reasonable amount of time to request that the school not disclose directory information about them. Schools must notify parents and eligible students annually of their rights under FERPA.[60]

Children's Online Privacy Protection Act (COPPA)

The Children's Online Privacy Protection Act (COPPA)[61] and its related rules regulate websites' collection and use of children's information. The operator of a website or online service that is directed to children, or that has actual knowledge that it collects children's personal information (covered entities), must comply with requirements regarding data collection and use, privacy policy notifications, and data security.

A covered entity may not collect a child's (individual under the age of 13) personal information without the prior, verifiable consent of his or her parent.[62]

COPPA requires covered entities to:[63]

---

[55] International Association of Privacy Processionals, *In Brief: The Financial Privacy Requirements of the Gramm-Leach-Bliley Act*, https://iapp.org/media/pdf/knowledge_center/brief_requirements_GLBA.pdf (last Jan. 28, 2022).
[56] 18 U.S.C. § 2721.
[57] Electronic Privacy Information Center, The Drivers Privacy Protection Act (DPPA) and the Privacy of Your State Motor Vehicle Record, https://epic.org/privacy/drivers/ (last visited Jan. 28, 2022).
[58] *Id*.
[59] 20 U.S.C. § 1232(g); 34 C.F.R. § 99.
[60] United States Department Of Education, Family Educational Rights and Privacy Act (FERPA), https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html (last visited Jan. 28, 2022).
[61] 16 C.F.R. pt. 312.
[62] 15 U.S.C. §§ 6502(a)-(b).

- Give parents direct notice of their privacy policies, including a description of their data collection and sharing practices;
- Post a clear link to their privacy policies on their home page and at each area of their website where they collect personal information from children;
- Institute procedures to protect the personal information that they hold;
- Ensure that any third party with which they share collected personal information implements the same protection procedures; and
- Delete children's personal information after the purpose for its retention has been fulfilled.

Violations of COPPA are deemed an unfair or deceptive act or practice and are therefore prosecuted by the FTC. COPPA also authorizes state attorneys general to enforce violations that affect residents of their states. There is no criminal prosecution or private right of action provided for under COPPA.[64]

Consumer Data Privacy – Effect of the Bill

Overview

The bill creates certain consumer rights related to personal information, including:
- The right to access personal information collected specific to the individual consumer,
- The right to delete or correct personal information, and
- The right to opt-out of the sale of sharing of personal information to third parties.

The bill defines "personal information" as information that identifies, relates to, or describes a particular consumer or household, or is reasonably capable of being directly or indirectly associated or linked with, a particular consumer or household. The term does not include public information from government records; or deidentified or aggregate consumer information.

A controller that receives a verifiable consumer request to access, delete, correct, or opt-out must comply with such consumer request, with certain exceptions. Exceptions include those for
- Certain small businesses;
- Businesses which only use personal information for marketing products or services it offers; and
- Businesses which only sell or share personal information under by certain federal privacy laws.

Controllers may share personal information with a processor, even if a consumer has "opted-out," if the processor processes information for a controller pursuant to a written contract which limits how the processor uses such information.

DLA may bring a FDUTPA action against a controller, processor, or person who violates the provisions of the bill, and such controller, processor, or person may be subject to certain civil penalties.

Exceptions

The bill does not apply to:
- Personal information collected and transmitted that is necessary for the sole purpose of sharing such personal information with a financial service provider to facilitate short term, transactional payment processing for the purchase of products or services.
- Deidentified personal information or aggregate consumer information.
- Compliance with federal, state, or local laws.
- Compliance with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities.

[63] *See*, Federal Trade Commission, *General Questions About the COPPA Rule: What is the Children's Online Privacy Protection Rule?*, https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0 (last visited Jan. 28, 2022).
[64] Federal Trade Commission, *General Questions About the COPPA Rule: COPPA Enforcement*, https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0 (last visited Jan. 28, 2022).

- Cooperation with law enforcement agencies concerning conduct or activity that the controller, processor, or third party reasonably and in good faith believes may violate federal, state, or local law.
- Exercising legal rights or privileges.
- Personal information used or collected by a controller or processor pursuant to a written contract between the controller and processor. Such information cannot be sold, shared, or disclosed to another person unless otherwise permitted.
- Personal information used by a controller or processor to advertise or market products or services that are produced or offered directly by the controller or processor as long as personal information is not sold, shared, or disclosed to another party outside the consumer's direct interaction with the controller or processor.
- Personal information collected by a controller of a natural person acting in the role of a job applicant, employee, owner, director, officer, contractor, volunteer, or intern of the controller, to the extent the personal information is collected and used solely within the context of the person's role or former role with the controller.
- Protected health information for purposes of HIPAA and related regulations, and patient identifying information for purposes of 42 C.F.R. Part 2, established pursuant to 42 U.S.C. s. 290dd-2.
- A covered entity or business associate governed by the privacy, security, and breach notification rules issued by the U.S. Department of Health and Human Services in 45 C.F.R. parts 160 and 164, or a program or a qualified service program defined in 42 C.F.R. part 2, to the extent the covered entity, business associate, or program maintains personal information in the same manner as medical information or protected health information and as long as the covered entity, business associate, or program does not use personal information for targeted advertising in conjunction with third parties and does not sell or share personal information to a third party unless such sale or sharing is covered by an exception.
- Identifiable private information collected for purposes of research as defined in 45 C.F.R. s. 164.501, conducted in accordance with the Federal Policy for the Protection of Human Subjects for purposes of 45 C.F.R. part 46, the good clinical practice guidelines issued by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use, the Protection for Human Subjects for purposes of 21 C.F.R. Parts 50 and 56; or personal information used or shared in research conducted in accordance with one or more of these standards.
- Information and documents created for purposes of the federal Health Care Quality Improvement Act of 1986 and related regulations, or patient safety work product for purposes of 42 C.F.R. part 3, established pursuant to 42 U.S.C. s. 299b-21 through 299b-26.
- Information that is deidentified in accordance with 45 C.F.R. part 164 and that is derived from individually identifiable health information, as described in HIPAA, or identifiable personal information, consistent with the Federal Policy for the Protection of Human Subjects or the human subject protection requirements of the FDA.
- Information used only for public health activities and purposes as described in 45 C.F.R. s. 164.512.
- Personal information collected, processed, sold, or disclosed pursuant to the federal Fair Credit Reporting Act, 15 U.S.C. s. 1681 and implementing regulations.
- Nonpublic personal information collected, processed, sold, or disclosed pursuant to the Gramm-Leach-Bliley Act, 15 U.S.C. s. 6801 et seq. and implementing regulations.
- A financial institution as defined in the Gramm-Leach-Bliley Act, 15 U.S.C. s. 6801 et seq. to the extent the financial institution maintains personal information in the same manner as nonpublic personal information, and as long as such financial institution does not use personal information for targeted advertising in conjunction with third parties and does not sell or share personal information to a third party unless such sale or sharing is covered by an exception.
- Personal information collected, processed, sold, or disclosed pursuant to the federal Driver's Privacy Protection Act of 1994, 18 U.S.C. s. 2721 et. seq.
- Education information covered by the Family Educational Rights and Privacy Act, 20 U.S.C. s. 1232(g) and 34 C.F.R. part 99.

- Information collected as part of public or peer-reviewed scientific or statistical research in the public interest.

Definitions

The bill includes the following definitions:

- "Aggregate consumer information".
- "Biometric information".
- "Collect".
- "Consumer" means a natural person who resides in or is domiciled in this state, however identified, including by any unique identifier.
- "Controller", which means:
    - A sole proprietorship, partnership, limited liability company, corporation, association, or legal entity that meets the following requirements:
        - Is organized or operated for the profit or financial benefit of its shareholders or owners;
        - Does business in this state;
        - Collects personal information about consumers, or is the entity on behalf of which such information is collected;
        - Determines the purposes and means of processing personal information about consumers alone or jointly with others; and
        - Satisfies two or more of the following thresholds:
            - Has global annual gross revenues in excess of $25 million, as adjusted in January of every odd-numbered year to reflect any increase in the Consumer Price Index.
            - Annually buys, receives, sells, or shares the personal information of 50,000 or more consumers, households, and devices for targeted advertising in conjunction with third parties or that is not covered by an exception.
            - Derives 50 percent or more of its global annual revenues from selling or sharing personal information about consumers.
    - Any entity that controls or is controlled by controller. As used in this definition, the term "control" means:
        - Ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a controller;
        - Control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or
        - The power to exercise a controlling influence over the management of a company.
- "Deidentified".
- "Department".
- "Device".
- "Homepage".
- "Household".
- "Personal information", which means information that is linked or reasonably linkable to an identified or identifiable consumer or household, including biometric information and unique identifiers to the consumer. The term does not include consumer information that is:
    - Publicly and lawfully made available.
    - Deidentified or aggregate consumer information.
    - Employment information.
- "Processing".
- "Processor", which means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that processes information on behalf of a controller and to which the controller discloses a consumer's personal information pursuant to a written contract, provided that the contract prohibits the entity receiving the information from

retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the controller, or as otherwise permitted.

- "Sell", which means to sell, rent, release, disclose, disseminate, make available, transfer, or otherwise communicate orally, in writing, or by electronic or other means, a consumer's personal information by a controller to another controller or a third party for monetary or other valuable consideration.
- "Share", which means to share, rent, release, disclose, disseminate, make available, transfer, or access a consumer's personal information for advertising. The term includes:
    - Allowing a third party to use or advertise to a consumer based on a consumer's personal information without disclosure of the personal information to the third party.
    - Monetary transactions, nonmonetary transactions, and transactions for other valuable consideration between a controller and a third party for advertising for the benefit of a controller.
- "Targeted advertising".
- "Third party".
- "Verifiable consumer request".

Consumer Data Collection Requirements and Responsibilities

The bill requires a controller that collects personal information about consumers to maintain an online privacy policy, make such policy available from its homepage. The online privacy policy must include the following information:

- Any Florida-specific consumer privacy rights.
- A list of the categories of personal information the controller collects or has collected about consumers.
- The right to request deletion or correction of certain personal information.
- The right to opt-out of the sale or sharing to third parties.

The bill requires a controller that collects personal information to, at or before the point of collection, inform consumers of the categories of personal information to be collected and the purposes for which the categories of personal information will be used.

The bill provides that a controller may not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with the requirements of the bill.

The bill provides that a controller that collects a consumer's personal information must implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure. A controller must require any processors and third parties to implement and maintain the same or similar security procedures and practices for personal information.

The bill requires a controller to adopt and implement a retention schedule that prohibits the use or retention of personal information by the controller or processor: after the satisfaction of the initial purpose for which such information was collected or obtained; after the expiration or termination of the contract pursuant to which the information was collected or obtained; or 3 years after the consumer's last interaction with the controller. The required retention schedule does not apply to personal information used or retained for the following purposes:

- Detection of security threats or incidents; protection against malicious, deceptive, fraudulent, unauthorized, or illegal activity or access; or prosecution of those responsible for such activity or access.
- Compliance with a legal obligation, including any federal retention laws.
- As reasonably needed for the protection of the controller's interests related to existing disputes, legal action, or governmental investigations.
- Assuring the physical security of persons or property.

Consumer Right to Request a Copy of Personal Information Collected, Sold, or Shared

The bill provides that a consumer has the right to request that a controller that collects personal information about the consumer disclose the personal information that has been collected, sold, or shared by or on behalf of the controller.

The bill provides that a consumer has the right to request that a controller that collects, sells, or shares personal information about the consumer to disclose the following to the consumer:

- The specific pieces of personal information that have been collected about the consumer.
- The sources from which the consumer's personal information was collected.
- The specific pieces of personal information about the consumer that were sold or shared.
- The third parties to which the personal information about the consumer was sold or shared.
- The categories of personal information about the consumer that were disclosed to a processor.

The bill requires a controller that collects, sells, or shares personal information about consumers to disclose the requested information to the consumer upon receipt of a verifiable consumer request.

The bill does not require a controller to retain, reidentify, or otherwise link any data that, in the ordinary course of business is not maintained in a manner that would be considered personal information.

The bill requires a controller to deliver the information required or act on a verifiable consumer request to a consumer free of charge within 45 days after receiving a verifiable consumer request. The response period may be extended once by 45 additional days when reasonably necessary, provided the controller informs the consumer of any such extension within the initial 45-day response period and the reason for the extension. The information must be delivered in a readily usable format. A controller is not obligated to provide information to the consumer if the consumer or a person authorized to act on the consumer's behalf does not provide verification of identity or verification of authorization to act with the permission of the consumer.

A controller may provide personal information to a consumer at any time, but may not be required to provide personal information to a consumer more than twice in a 12-month period.

Such requirements to disclose information do not apply to personal information relating solely to households.

Consumer Right to Correct or Delete Personal Information

The bill provides that consumer has the right to request that a controller delete any personal information about the consumer which the controller has collected from the consumer.

The bill requires a controller that receives a verifiable consumer request to delete the consumer's personal information to delete the consumer's personal information from its records and direct any processors to delete such information within 90 days of receipt of the verifiable consumer request.

A controller or a processor acting pursuant to its contract with the controller may not be required to comply with a consumer's request to delete the consumer's personal information if it is reasonably necessary for the controller or processor to maintain the consumer's personal information to do any of the following:

- Complete the transaction for which the personal information was collected.
- Fulfill the terms of a written warranty or product recall conducted in accordance with federal law.
- Provide a good or service requested by the consumer, or reasonably anticipated to be requested within the context of a controller's ongoing business relationship with the consumer, or otherwise perform a contract between the controller and the consumer.
- Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity.
- Debug to identify and repair errors that impair existing intended functionality.

- Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws when the controller's deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent.
- Enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the controller or that are compatible with the context in which the consumer provided the information.
- Comply with a legal obligation, including any state or federal retention laws.
- Reasonably protect the controller's interests against existing disputes, legal action, or governmental investigations.
- Internally use the consumer's personal information in a lawful manner.

The bill allows a consumer to make a request to correct inaccurate personal information to a controller that maintains inaccurate personal information about the consumer. A controller that receives a verifiable consumer request to correct inaccurate personal information must use commercially reasonable efforts to correct the inaccurate personal information as directed by the consumer and direct any processors to correct such information within 90 days after receipt of the verifiable consumer request. If a controller maintains a self-service mechanism to allow a consumer to correct certain personal information, the controller may require the consumer to correct their own personal information through such mechanism.

Consumer Right to Opt-Out of the Sale or Sharing of Personal Information

The bill provides that a consumer has the right at any time to direct a controller that sells or shares personal information about the consumer to third parties to not sell or share the consumer's personal information. This right may be referred to as the right to opt-out.

The bill requires that a controller that sells or shares personal information to third parties to provide notice to consumers that this information may be sold and shared and that consumers have the right to opt-out of the sale or sharing of their personal information.

The bill provides that a controller may not sell or share the personal information of a minor consumer if the controller has actual knowledge that the consumer is not 16 years of age or older. However, if a consumer who is between 13 and 16 years of age, or if the parent or guardian of a consumer who is 12 years of age or younger, has affirmatively authorized the sale or sharing of such consumer's personal information, then a controller may sell or share such information. A controller that willfully disregards the consumer's age is deemed to have actual knowledge of the consumer's age. A controller that complies with the verifiable parental consent requirements of COPPA is deemed compliant with any obligation to obtain parental consent.

The bill provides that a controller that has received direction prohibiting the sale or sharing of the consumer's personal information is prohibited from selling or sharing the consumer's personal information beginning 48 hours after receipt of such direction, unless the consumer subsequently provides express authorization for the sale or sharing of the consumer's personal information.

Form to Opt-Out of the Sale or Sharing of Personal Information

The bill requires a controller, in a reasonably accessible format, to provide a clear and conspicuous link on the controller's Internet homepage, entitled "Do Not Sell or Share My Personal Information," to an Internet webpage that enables a consumer, or a person authorized by the consumer, to opt-out of the sale or sharing of the consumer's personal information. A controller may not require a consumer to create an account in order to direct the controller not to sell the consumer's personal information.

A controller may accept a request to opt-out received through a user-enabled global privacy control, such as a browser plug-in or privacy setting, device setting, or other mechanism, which communicates or signals the consumer's choice to opt out.

A controller must respect the consumer's decision to opt-out for at least 12 months before requesting that the consumer authorize the sale or sharing of the consumer's personal information.

A controller may not use any personal information collected from the consumer in connection with the submission of the consumer's opt-out request solely for the purposes of complying with the opt-out request.

The bill allows a consumer to authorize another person to opt-out of the sale or sharing of the consumer's personal information on the consumer's behalf, and a controller must comply with an opt-out request received from a person authorized by the consumer to act on the consumer's behalf, pursuant to rules adopted by DLA.

Actions Related to Consumers Who Exercise Their Rights

The bill allows a controller to charge a consumer who exercised any of the consumer's rights a different price or rate, or provide a different level or quality of goods or services to the consumer, but only if that difference is:

- Reasonably related to the value provided to the controller by the consumer's data, or
- Related to a consumer's voluntary participation in a financial incentive program, including a bona fide loyalty, rewards, premium features, discounts, or club card program offered by the controller.

A controller may offer financial incentives, including payments to consumers as compensation, for the collection, sharing, sale, or deletion of personal information if the consumer gives the controller prior consent that clearly describes the material terms of the financial incentive program. The consent may be revoked by the consumer at any time.

The bill prohibits a controller from using financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature.

Contracts and Roles

The bill requires that any contract between a controller and a processor must:

- Prohibit the processor from selling, sharing, retaining, using, or disclosing the personal information other than for the purposes specified in the contract or agreement with the controller;
- Govern the processor's personal information processing procedures with respect to processing performed on behalf of the controller, including processing instructions, the nature and purpose of processing, the type of information subject to processing, the duration of processing, and the rights and obligations of both the controller and processor;
- Require the processor to return or delete all personal information under the contract to the controller as requested by the controller at the end of the provision of services, unless retention of the information is required by law; and
- Upon request of the controller, require the processor to make available to the controller all information in its possession under the contract or agreement.

The bill provides that determining whether a person is acting as a controller or processor with respect to a specific processing of data is fact-based and depends upon the context in which personal information is to be processed. The contract between a controller and processor must reflect their respective roles and relationships related to handling personal information. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal information remains a processor.

The bill provides that a third party may not sell or share personal information about a consumer that has been sold or shared to the third party by a controller unless the consumer has received explicit notice from the third party and is provided an opportunity to opt-out by the third party.

The bill requires a third party or a processor to require any subcontractor to meet the same obligations of such third party or processor with respect to personal information.

Any provision of a contract or agreement that waives or limits in any way a consumer's rights under the bill, including, but not limited to, any right to a remedy or means of enforcement, is deemed contrary to public policy and is void and unenforceable.

Private Causes of Action

The bill allows a Florida consumer to bring a civil action against a controller, processor, or person for the following:

- Failure to delete or correct a consumer's personal information after receiving a verifiable consumer request, unless the controller qualifies for an exception to requirements to delete or correct;
- Continuing to sell or share a consumer's personal information after the consumer chooses to opt-out; or
- Selling or sharing the personal information of a consumer age 16 or younger without obtaining required consent.

The bill allows a court to grant the following relief to a consumer:

- Damages in an amount not less than $100 and not greater than $750 per consumer per incident, or actual damages, whichever is greater.
- Injunctive or declaratory relief.
- Upon prevailing in a civil action, the consumer may recover reasonable attorney's fees and costs.

Except as authorized under the private cause of action or the DLA enforcement provisions, liability for a tort, contract claim, or consumer protection claim does not arise solely from the failure of a controller, processor, or person to comply with the bill. Evidence of such may only be used as the basis to prove a cause of action under the bill.

Enforcement and Implementation

The bill provides that if DLA has reason to believe that any controller, processor, or person is in violation of the requirements of the bill, DLA may bring an action against such controller, processor, or person for an unfair or deceptive act or practice under FDUTPA. A consumer may not bring an action under FDUTPA under the bill. DLA is permitted to bring an action against:

- Any person or activity regulated under laws administered by the Office of Insurance Regulation or the Department of Financial Services; and
- Banks, credit unions, and savings and loan associations regulated by the Office of Financial Regulation or federal agencies.

Civil penalties may be tripled if the violation involves a consumer who the controller, processor or person has actual knowledge is 16 years of age or younger, or if the basis of the complaint is one of the instances where an individual consumer may bring a private cause of action.

After the DLA has notified a controller, processor, or person in writing of an alleged violation, the DLA may, in its discretion, grant the controller, processor, or person a 45-day period to cure the alleged violation. The DLA may consider the number of violations, the substantial likelihood of injury to the public, or the safety of persons or property when determining whether to grant 45 days to cure. If the controller, processor, or person cures the alleged violation to the satisfaction of the DLA and provides proof to the DLA, the DLA may issue a letter of guidance. If the controller, processor, or person fails to cure the violation to the satisfaction of the DLA within 45 days, the DLA may bring an action against the controller, processor, or person for the alleged violation.

The bill clarifies that any action brought by DLA may only be brought by or on behalf of a Florida consumer.

DLA may adopt rules to implement the bill, including standards for verifiable consumer requests, enforcement, data security, and authorized persons who may act on a consumer's behalf.

The bill requires DLA to submit a report by February 1 each year to the President of the Senate and the Speaker of the House of Representatives describing any actions taken by DLA to enforce the bill. The report must include statistics and relevant information detailing:

- The number of complaints received;
- The number and type of enforcement actions taken and the outcomes of such actions;
- The number of complaints resolved without the need for litigation; and
- The status of the development and implementation of rules to implement the bill.

Jurisdiction

For purposes of bringing an action under the bill, any controller that collects, shares, or sells the personal information of a Florida consumer, is considered to be both engaged in substantial and not isolated activities within this state, and is operating, conducting, engaging in, or carrying on a business, and doing business in this state, and is therefore subject to the jurisdiction of Florida courts.

Preemption

The bill provides that consumer data privacy is a matter of statewide concern and he bill supersedes all rules, regulations, codes, ordinances, and other laws adopted by a city, county, city and county, municipality, or local agency regarding the collection, processing, sharing, or sale of consumer personal information by a controller or processor. The regulation of the collection, processing, sharing, or sale of consumer personal information by a controller or processor is preempted to the state.

Florida Information Protection Act – Current Situation

In 2014, Florida passed the Florida Information Protection Act (FIPA).[65] FIPA requires commercial covered entities[66] and government entities which hold personal information to take reasonable measures to protect such information and report data breaches to affected consumers.[67]

FIPA defines "personal information" as:

- Online account information, such as security questions and answers, email addresses and passwords;
- An individual's first name or first initial and last name in combination with any one or more of the following:
    - A social security number;
    - A driver license or similar identity verification number issued on a government document;
    - A financial account number or credit 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;
    - Any medical history information; or
    - An individual's health insurance identification numbers.[68]

Personal information does not include information:

- About an individual that has been made publicly available by a federal, state, or local governmental entity; or

[65] S. 501.171, F.S.; Fla. SB 1524 (2014) (FIPA expanded and updated Florida's data breach disclosure laws contained in s. 817.56 81, F.S. (2013), which was adopted in 2005 and repealed in 2014.)
[66] "Covered entity" means a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other com mercial entity that acquires, maintains, stores, or uses personal information. S. 501.171(1)(b), F.S.
[67] Florida Office of the Attorney General, *How to Protect Yourself: Data Security*, http://myfloridalegal.com/pages.nsf/Main/53D4216591361BCD85257F77004BE16C (last visited Jan. 28, 2022).
[68] *Id*.; S. 501.171(1)(g)1., F.S.

- That is encrypted, secured, or modified to remove elements that personally identify an individual or that otherwise renders the information unusable.[69]

If a breach of personal information occurs, notice must be given to each individual in this state whose personal information was accessed as a result of the breach. If the breach affected 500 or more individuals in this state, the covered entity must also provide notice to the Department of Legal Affairs (DLA). If the breach affected more than 1,000 individuals at a single time, credit reporting agencies must be notified of such breach, with certain exceptions.[70]

FIPA expressly does not provide a private cause of action, but does authorize enforcement actions by DLA under Florida's Unfair and Deceptive Trade Practices Act (FDUTPA) against covered entities for any statutory violations.[71]

In addition to the remedies provided for under FDUTPA, a covered entity that fails to notify DLA, or an individual whose personal information was accessed, of the data breach is liable for a civil penalty not to exceed $500,000:

- In the amount of $1,000 for each day up to the first 30 days following any violation, thereafter, $50,000 for each subsequent 30-day period or portion thereof for up to 180 days.
- If the violation continues for more than 180 days, in an amount not to exceed $500,000.

The civil penalties for failure to notify apply per breach and not per individual affected by the breach.

Florida Information Protection Act – Effect of the Bill

The bill defines **"Biometric data"** as an individual's physiological, biological, or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. The term includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.

The bill includes biometric data in FIPA's definition of "personal information" so that covered entities are required to notify the affected individual, the DLA, and credit reporting agencies of a breach of biometric information paired with an individual's first name or first initial and last name.

The bill allows DLA to bring a FDUTPA action against a covered entity which fails to notify DLA of or an individual affected by a breach of biometric information.

The bill provides an effective date of July 1, 2023.

B. SECTION DIRECTORY:

Section 1: Creates s. 501.173, F.S., relating to consumer data privacy rights and requirements.
Section 2: Amends s. 501.171, F.S.; relating to FIPA and triggering requirements.
Section 3: Provides an effective date.

II. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT

A. FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues:

There may be an increase in civil penalties collected by DLA.

[69] S. 501.171(1)(g)2., F.S.
[70] S. 501.171(3)-(6), F.S.
[71] S. 501.171(9), (10), F.S.; OAG *supra* note 66.

2. Expenditures:

There may be an increase of regulatory costs to DLA from implementing and enforcing the bill.

B. FISCAL IMPACT ON LOCAL GOVERNMENTS:

1. Revenues:

None.

2. Expenditures:

None.

C. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR:

The bill will require certain businesses in possession of personal information to implement mechanisms to effectuate the requirements of the bill, and such implementation will have a fiscal impact on such businesses. However, many of the businesses subject to the bill's requirements have already implemented similar privacy practices based on protections required in other states and countries.

It may increase protections provided for personal information that may save consumers the expense of dealing with stolen personal information used to commit financial crimes. Some 15 million consumers are victims of identity theft or fraud a year. Identity theft and fraud costs consumers more than $15 billion a year.

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:

DLA is given rulemaking authority in the bill to implement the bill.

C. DRAFTING ISSUES OR OTHER COMMENTS:

None.

IV. AMENDMENTS/COMMITTEE SUBSTITUTE CHANGES

A bill to be entitled

An act relating to consumer data privacy; creating s. 501.173, F.S.; providing applicability; providing definitions; requiring controllers that collect a consumer's personal data to disclose certain information regarding data collection and selling practices to the consumer at or before the point of collection; specifying that such information may be provided through a general privacy policy or through a notice informing the consumer that additional specific information will be provided upon a certain request; prohibiting controllers from collecting additional categories of personal information or using personal information for additional purposes without notifying the consumer; requiring controllers that collect personal information to implement reasonable security procedures and practices to protect the information; authorizing consumers to request controllers to disclose the specific personal information the controller has collected about the consumer; requiring controllers to make available two or more methods for consumers to request their personal information; requiring controllers to provide such information free of charge within a certain timeframe and in a certain format upon receiving a verifiable consumer request;

specifying requirements for third parties with respect to consumer information acquired or used; providing construction; authorizing consumers to request controllers to delete or correct personal information the controllers have collected about the consumers; providing exceptions; specifying requirements for controllers to comply with deletion or correction requests; authorizing consumers to opt out of third-party disclosure of personal information collected by a controller; prohibiting controllers from selling or disclosing the personal information of consumers younger than a certain age, except under certain circumstances; prohibiting controllers from selling or sharing a consumer's information if the consumer has opted out of such disclosure; prohibiting controllers from taking certain actions to retaliate against consumers who exercise certain rights; providing applicability; providing that a contract or agreement that waives or limits certain consumer rights is void and unenforceable; providing for civil actions and a private right of action for consumers under certain circumstances; providing civil remedies; authorizing the Department of Legal Affairs to bring an action under the Florida Unfair or Deceptive Trade Practices Act and to adopt rules; requiring the department to

submit an annual report to the Legislature; providing report requirements; providing that controllers must have a specified timeframe to cure any violations; providing jurisdiction; declaring that the act is matter of statewide concern; preempting the collection, processing, sharing, and sale of consumer personal information to the state; amending s. 501.171, F.S.; revising the definition of "personal information"; providing an effective date.

Be It Enacted by the Legislature of the State of Florida:

Section 1. Section 501.173, Florida Statutes, is created to read:

501.173 Consumer data privacy.—

(1) APPLICABILITY.—This section does not apply to:

(a) Personal information collected and transmitted that is necessary for the sole purpose of sharing such personal information with a financial service provider to facilitate short term, transactional payment processing for the purchase of products or services.

(b) Personal information collected, used, retained, sold, shared, or disclosed as deidentified personal information or aggregate consumer information.

(c) Compliance with federal, state, or local laws.

(d) Compliance with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities.

(e) Cooperation with law enforcement agencies concerning conduct or activity that the controller, processor, or third party reasonably and in good faith believes may violate federal, state, or local law.

(f) Exercising legal rights or privileges.

(g) Personal information used or collected by a controller or processor pursuant to a written contract between the controller and processor that complies with the requirements of this section.

(h) Personal information used by a controller or processor to advertise or market products or services that are produced or offered directly by the controller or processor. Such information may not be sold, shared, or disclosed to another person unless otherwise authorized under this section.

(i) Personal information of a person acting in the role of a job applicant, employee, owner, director, officer, contractor, volunteer, or intern of a controller, that is collected by a controller, to the extent the personal information is collected and used solely within the context of the person's role or former role with the controller.

(j) Protected health information for purposes of the federal Health Insurance Portability and Accountability Act of

1996 and related regulations, and patient identifying information for purposes of 42 C.F.R. part 2, established pursuant to 42 U.S.C. s. 290dd-2.

(k) A covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services in 45 C.F.R. parts 160 and 164, or a program or a qualified service program as defined in 42 C.F.R. part 2, to the extent the covered entity, business associate, or program maintains personal information in the same manner as medical information or protected health information as described in paragraph (j), and as long as the covered entity, business associate, or program does not use personal information for targeted advertising with third parties and does not sell or share personal information to a third party unless such sale or sharing is covered by an exception under this section.

(l) Identifiable private information collected for purposes of research as defined in 45 C.F.R. s. 164.501 conducted in accordance with the Federal Policy for the Protection of Human Subjects for purposes of 45 C.F.R. part 46, the good clinical practice guidelines issued by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use, or the Protection for Human Subjects for purposes of 21 C.F.R. parts 50 and 56, or personal information that is used or shared in

research conducted in accordance with one or more of these standards.

(m) Information and documents created for purposes of the federal Health Care Quality Improvement Act of 1986 and related regulations, or patient safety work product for purposes of 42 C.F.R. part 3, established pursuant to 42 U.S.C. s. 299b-21 through 299b-26.

(n) Information that is deidentified in accordance with 45 C.F.R. part 164 and derived from individually identifiable health information as described in the Health Insurance Portability and Accountability Act of 1996, or identifiable personal information, consistent with the Federal Policy for the Protection of Human Subjects or the human subject protection requirements of the United States Food and Drug Administration.

(o) Information used only for public health activities and purposes as described in 45 C.F.R. s. 164.512.

(p) Personal information collected, processed, sold, or disclosed pursuant to the federal Fair Credit Reporting Act, 15 U.S.C. s. 1681 and implementing regulations.

(q) Nonpublic personal information collected, processed, sold, or disclosed pursuant to the Gramm-Leach-Bliley Act, 15 U.S.C. s. 6801 et seq., and implementing regulations.

(r) A financial institution as defined in the Gramm-Leach-Bliley Act, 15 U.S.C. s. 6801 et seq., to the extent the financial institution maintains personal information in the same

manner as nonpublic personal information as described in paragraph (q), and as long as such financial institution does not use personal information for targeted advertising with third parties and does not sell or share personal information to a third party unless such sale or sharing is covered by an exception under this section.

(s) Personal information collected, processed, sold, or disclosed pursuant to the federal Driver's Privacy Protection Act of 1994, 18 U.S.C. s. 2721 et seq.

(t) Education information covered by the Family Educational Rights and Privacy Act, 20 U.S.C. s. 1232(g) and 34 C.F.R. part 99.

(u) Information collected as part of public or peer-reviewed scientific or statistical research in the public interest and that adheres to all other applicable ethics and privacy laws, if the consumer has provided informed consent. Research with personal information must be subjected by the controller conducting the research to additional security controls that limit access to the research data to only those individuals necessary to carry out the research purpose and subsequently deidentified.

(v) Personal information disclosed for the purpose of responding to an alert of a present risk of harm to a person or property, detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, or

prosecuting those responsible for that activity.

(w) Personal information that is disclosed when a consumer uses or directs a controller to intentionally disclose information to a third party or uses the controller to intentionally interact with a third party. An intentional interaction occurs when the consumer intends to interact with the third party, by one or more deliberate interactions. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer's intent to interact with a third party.

(x) An identifier used for a consumer who has opted out of the sale or sharing of the consumer's personal information for the sole purpose of alerting processors and third parties that the consumer has opted out of the sale or sharing of the consumer's personal information.

(y) Personal information transferred by a controller to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller, provided that information is used or shared consistently with this section. If a third party materially alters how it uses or shares the personal information of a consumer in a manner that is materially inconsistent with the commitments or promises made at the time of collection, it shall provide prior notice of the new or changed practice to the consumer. The notice must be

sufficiently prominent and robust to ensure that consumers can easily exercise choices consistent with this section.

(2) DEFINITIONS.—As used in this section, the term:

(a) "Aggregate consumer information" means information that relates to a group or category of consumers, from which the identity of an individual consumer has been removed and is not reasonably capable of being directly or indirectly associated or linked with, any consumer, household, or device. The term does not include personal information that has been deidentified.

(b) "Biometric information" means an individual's physiological, biological, or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. The term includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.

(c) "Collect" means to buy, rent, gather, obtain, receive, or access any personal information pertaining to a consumer by any means. The term includes, but is not limited to, actively or passively receiving information from the consumer or by

observing the consumer's behavior or actions.

(d) "Consumer" means a natural person who resides in or is domiciled in this state, however identified, including by any unique identifier, who is acting in a personal capacity or household context. The term does not include a natural person acting on behalf of a legal entity in a commercial or employment context.

(e) "Controller" means:

1. A sole proprietorship, partnership, limited liability company, corporation, association, or legal entity that meets the following requirements:

a. Is organized or operated for the profit or financial benefit of its shareholders or owners;

b. Does business in this state;

c. Collects personal information about consumers, or is the entity on behalf of which such information is collected;

d. Determines the purposes and means of processing personal information about consumers alone or jointly with others; and

e. Satisfies at least two of the following thresholds:

(I) Has global annual gross revenues in excess of $50 million, as adjusted in January of every odd-numbered year to reflect any increase in the Consumer Price Index.

(II) Annually buys, receives, sells, or shares the personal information of 50,000 or more consumers, households, or

devices for the purpose of targeted advertising in conjunction with third parties or for a purpose that is not listed under subsection (1).

(III) Derives 50 percent or more of its global annual revenues from selling or sharing personal information about consumers.

2. Any entity that controls or is controlled by a controller. As used in this subparagraph, the term "control" means:

a. Ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a controller;

b. Control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or

c. The power to exercise a controlling influence over the management of a company.

(f) "Deidentified" means information that cannot reasonably be used to infer information about or otherwise be linked to a particular consumer, provided that the controller that possesses the information:

1. Takes reasonable measures to ensure that the information cannot be associated with a specific consumer;

2. Maintains and uses the information in deidentified form and not to attempt to reidentify the information, except that

the controller may attempt to reidentify the information solely for the purpose of determining whether its deidentification processes satisfy the requirements of this paragraph; and

3. Contractually obligates any recipients of the information to comply with all the provisions of this paragraph to avoid reidentifying such information.

(g) "Department" means the Department of Legal Affairs.

(h) "Device" means a physical object associated with a consumer or household capable of directly or indirectly connecting to the Internet.

(i) "Homepage" means the introductory page of an Internet website and any Internet webpage where personal information is collected. In the case of a mobile application, the homepage is the application's platform page or download page, a link within the application, such as the "About" or "Information" application configurations, or settings page, and any other location that allows consumers to review the notice required by subsection (7), including, but not limited to, before downloading the application.

(j) "Household" means a natural person or a group of people in this state who reside at the same address, share a common device or the same service provided by a controller, and are identified by a controller as sharing the same group account or unique identifier.

(k) "Personal information" means information that is

linked or reasonably linkable to an identified or identifiable consumer or household, including biometric information and unique identifiers to the consumer. The term does not include consumer information that is:

1. Consumer employment contact information, including a position name or title, employment qualifications, emergency contact information, business telephone number, business electronic mail address, employee benefit information, and similar information used solely in an employment context.

2. Deidentified or aggregate consumer information.

3. Publicly and lawfully available information reasonably believed to be made available to the public in a lawful manner and without legal restrictions:

a. From federal, state, or local government records.

b. By a widely distributed media source.

c. By the consumer or by someone to whom the consumer disclosed the information unless the consumer has purposely and effectively restricted the information to a certain audience on a private account.

(l) "Processing" means any operation or set of operations that are performed on personal information or on sets of personal information, whether or not by automated means.

(m) "Processor" means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or

financial benefit of its shareholders or other owners, that processes information on behalf of a controller and to which the controller discloses a consumer's personal information pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the controller, or as otherwise permitted by this section.

(n) "Sell" means to sell, rent, release, disclose, disseminate, make available, transfer, or otherwise communicate orally, in writing, or by electronic or other means, a consumer's personal information by a controller to another controller or a third party for monetary or other valuable consideration.

(o) "Share" means to share, rent, release, disclose, disseminate, make available, transfer, or access a consumer's personal information for advertising or marketing. The term includes:

1. Allowing a third party to use or advertise or market to a consumer based on a consumer's personal information without disclosure of the personal information to the third party.

2. Monetary transactions, nonmonetary transactions, and transactions for other valuable consideration between a controller and a third party for advertising or marketing for

the benefit of a controller.

(p) "Targeted advertising" means marketing to a consumer or displaying an advertisement to a consumer when the advertisement is selected based on personal information used to predict such consumer's preferences or interests.

(q) "Third party" means a person who is not a controller or processor.

(r) "Verifiable consumer request" means a request related to personal information that is made by a consumer, by a parent or guardian on behalf of a consumer who is a minor child, or by a person authorized by the consumer to act on the consumer's behalf in a form that is reasonably and readily accessible to consumers and that the controller can reasonably verify to be the consumer pursuant to rules adopted by the department.

(3) CONSUMER DATA COLLECTION REQUIREMENTS AND RESPONSIBILITIES.—

(a) A controller that collects personal information about consumers shall maintain an up-to-date online privacy policy and make such policy available from its homepage. The online privacy policy must include the following information:

1. Any Florida-specific consumer privacy rights.

2. A list of the types and categories of personal information the controller collects, sells, or shares, or has collected, sold, or shared, about consumers.

3. The consumer's right to request deletion or correction

of certain personal information.

4. The consumer's right to opt-out of the sale or sharing to third parties.

(b) A controller that collects personal information shall, at or before the point of collection, inform, or direct the processor to inform, consumers of the categories of personal information to be collected and the purposes for which the categories of personal information will be used.

(c) A controller may not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section.

(d) A controller that collects a consumer's personal information shall implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure. A controller must require any processors and third parties to implement and maintain the same or similar security procedures and practices for personal information.

(e) A controller shall adopt and implement a retention schedule that prohibits the use or retention of personal information not subject to an exemption by the controller or processor after the satisfaction of the initial purpose for which such information was collected or obtained, after the

expiration or termination of the contract pursuant to which the information was collected or obtained, or 3 years after the consumer's last interaction with the controller. This paragraph does not apply to personal information used or retained for the following purposes:

1. Detection of security threats or incidents; protection against malicious, deceptive, fraudulent, unauthorized, or illegal activity or access; or prosecution of those responsible for such activity or access.

2. Compliance with a legal obligation, including any federal retention laws.

3. As reasonably needed for the protection of the controller's interests related to existing disputes, legal action, or governmental investigations.

4. Assuring the physical security of persons or property.

(4) CONSUMER RIGHT TO REQUEST COPY OF PERSONAL DATA COLLECTED, SOLD, OR SHARED.—

(a) A consumer has the right to request that a controller that collects, sells, or shares personal information about the consumer to disclose the following to the consumer:

1. The specific pieces of personal information that have been collected about the consumer.

2. The sources from which the consumer's personal information was collected.

3. The specific pieces of personal information about the

consumer that were sold or shared.

4. The third parties to which the personal information about the consumer was sold or shared.

5. The categories of personal information about the consumer that were disclosed to a processor.

(b) A controller that collects, sells, or shares personal information about a consumer shall disclose the information specified in paragraph (a) to the consumer upon receipt of a verifiable consumer request.

(c) This subsection does not require a controller to retain, reidentify, or otherwise link any data that, in the ordinary course of business is not maintained in a manner that would be considered personal information.

(d) The controller shall deliver the information required or act on the request in this subsection to a consumer free of charge within 45 days after receiving a verifiable consumer request. The response period may be extended once by 45 additional days when reasonably necessary, provided the controller informs the consumer of any such extension within the initial 45-day response period and the reason for the extension. The information must be delivered in a readily usable format. A controller is not obligated to provide information to the consumer if the consumer or a person authorized to act on the consumer's behalf does not provide verification of identity or verification of authorization to act with the permission of the

consumer.

(e) A controller may provide personal information to a consumer at any time, but is not required to provide personal information to a consumer more than twice in a 12-month period.

(f) This subsection does not apply to personal information relating solely to households.

(5) RIGHT TO HAVE PERSONAL INFORMATION DELETED OR CORRECTED.—

(a) A consumer has the right to request that a controller delete any personal information about the consumer which the controller has collected from the consumer.

(b) A controller that receives a verifiable consumer request to delete the consumer's personal information shall delete the consumer's personal information from its records and direct any processors to delete such information within 90 days of receipt of the verifiable consumer request.

(c) A controller or a processor acting pursuant to its contract with the controller may not be required to comply with a consumer's request to delete the consumer's personal information if it is reasonably necessary for the controller or processor to maintain the consumer's personal information to do any of the following:

1. Complete the transaction for which the personal information was collected.

2. Fulfill the terms of a written warranty or product

recall conducted in accordance with federal law.

3. Provide a good or service requested by the consumer, or reasonably anticipated to be requested within the context of a controller's ongoing business relationship with the consumer, or otherwise perform a contract between the controller and the consumer.

4. Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity.

5. Debug to identify and repair errors that impair existing intended functionality.

6. Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws when the controller's deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent.

7. Enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the controller or that are compatible with the context in which the consumer provided the information.

8. Comply with a legal obligation, including any state or federal retention laws.

9. Reasonably protect the controller's interests against existing disputes, legal action, or governmental investigations.

10. Internally use the consumer's personal information in a lawful manner.

(d) A consumer has the right to make a request to correct inaccurate personal information to a controller that maintains inaccurate personal information about the consumer. A controller that receives a verifiable consumer request to correct inaccurate personal information shall use commercially reasonable efforts to correct the inaccurate personal information as directed by the consumer and direct any processors to correct such information within 90 days after receipt of the verifiable consumer request. If a controller maintains a self-service mechanism to allow a consumer to correct certain personal information, the controller may require the consumer to correct their own personal information through such mechanism.

(6) RIGHT TO OPT-OUT OF THE SALE OR SHARING OF PERSONAL INFORMATION.—

(a) A consumer has the right at any time to direct a controller not to sell or share the consumer's personal information to a third party. This right may be referred to as the right to opt-out.

(b) Notwithstanding paragraph (a), a controller may not sell or share the personal information of a minor consumer if the controller has actual knowledge that the consumer is not 16 years of age or older. However, if a consumer who is between 13

and 16 years of age, or if the parent or guardian of a consumer who is 12 years of age or younger, has affirmatively authorized the sale or sharing of such consumer's personal information, then a controller may sell or share such information in accordance with this section. A controller that willfully disregards the consumer's age is deemed to have actual knowledge of the consumer's age. A controller that complies with the verifiable parental consent requirements of the Children's Online Privacy Protection Act, 15 U.S.C. s. 6501 et seq., shall be deemed compliant with any obligation to obtain parental consent.

(c) A controller that has received direction prohibiting the sale or sharing of the consumer's personal information is prohibited from selling or sharing the consumer's personal information beginning 48 hours after receipt of such direction, unless the consumer subsequently provides express authorization for the sale or sharing of the consumer's personal information.

(7) FORM TO OPT-OUT OF SALE OR SHARING OF PERSONAL INFORMATION.—

(a) A controller shall:

1. In a form that is reasonably accessible to consumers, provide a clear and conspicuous link on the controller's Internet homepage, entitled "Do Not Sell or Share My Personal Information," to an Internet webpage that enables a consumer, or a person authorized by the consumer, to opt-out of the sale or

sharing of the consumer's personal information. A controller may not require a consumer to create an account in order to direct the controller not to sell the consumer's personal information. A controller may accept a request to opt-out received through a user-enabled global privacy control, such as a browser plug-in or privacy setting, device setting, or other mechanism, which communicates or signals the consumer's choice to opt out.

2. For consumers who opted-out of the sale or sharing of their personal information, respect the consumer's decision to opt-out for at least 12 months before requesting that the consumer authorize the sale or sharing of the consumer's personal information.

3. Use any personal information collected from the consumer in connection with the submission of the consumer's opt-out request solely for the purposes of complying with the opt-out request.

(b) A consumer may authorize another person to opt-out of the sale or sharing of the consumer's personal information on the consumer's behalf pursuant to rules adopted by the department.

(8) ACTIONS RELATED TO CONSUMERS WHO EXERCISE PRIVACY RIGHTS.—

(a) A controller may charge a consumer who exercised any of the consumer's rights under this section a different price or rate, or provide a different level or quality of goods or

services to the consumer, only if that difference is reasonably related to the value provided to the controller by the consumer's data or is related to a consumer's voluntary participation in a financial incentive program, including a bona fide loyalty, rewards, premium features, discounts, or club card program offered by the controller.

(b) A controller may offer financial incentives, including payments to consumers as compensation, for the collection, sharing, sale, or deletion of personal information if the consumer gives the controller prior consent that clearly describes the material terms of the financial incentive program. The consent may be revoked by the consumer at any time.

(c) A controller may not use financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature.

(9) CONTRACTS AND ROLES.—

(a) Any contract or agreement between a controller and a processor must:

1. Prohibit the processor from selling, sharing, retaining, using, or disclosing the personal information other than for the purposes specified in the contract or agreement with the controller;

2. Govern the processor's personal information processing procedures with respect to processing performed on behalf of the controller, including processing instructions, the nature and purpose of processing, the type of information subject to

processing, the duration of processing, and the rights and obligations of both the controller and processor;

3. Require the processor to return or delete all personal information under the contract to the controller as requested by the controller at the end of the provision of services, unless retention of the information is required by law; and

4. Upon request of the controller, require the processor to make available to the controller all information in its possession under the contract or agreement.

(b) Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal information is to be processed. The contract between a controller and processor must reflect their respective roles and relationships related to handling personal information. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal information remains a processor.

(c) A third party may not sell or share personal information about a consumer that has been sold or shared to the third party by a controller unless the consumer has received explicit notice from the third party and is provided an opportunity to opt-out by the third party.

(d) A processor or third party must require any subcontractor to meet the same obligations of such processor or

third party with respect to personal information.

(e) A processor or third party or any subcontractor thereof who violates any of the restrictions imposed upon it under this section is liable or responsible for any failure to comply with this section.

(f) Any provision of a contract or agreement of any kind that waives or limits in any way a consumer's rights under this section, including, but not limited to, any right to a remedy or means of enforcement, is deemed contrary to public policy and is void and unenforceable. This section does not prevent a consumer from declining to request information from a controller, declining to opt-out of a controller's sale or sharing of the consumer's personal information, or authorizing a controller to sell or share the consumer's personal information after previously opting out.

(10) CIVIL ACTIONS; PRIVATE RIGHT OF ACTION.—

(a) A Florida consumer may only bring a civil action against a controller, processor, or person pursuant to this section for the following:

1. Failure to delete or correct a consumer's personal information pursuant to this section after receiving a verifiable consumer request or directions to delete or correct from a controller unless the controller, processor, or person qualifies for an exception to the requirements to delete or correct under this section.

2. Continuing to sell or share a consumer's personal information after the consumer chooses to opt-out pursuant to this section.

3. Selling or sharing the personal information of a consumer age 16 or younger without obtaining consent as required by this section.

(b) A court may grant the following relief to a consumer:

1. Damages in an amount not less than $100 and not greater than $750 per consumer per incident or actual damages, whichever is greater.

2. Injunctive or declaratory relief.

(c) Upon prevailing, the consumer shall recover reasonable attorney fees and costs.

(d) Any action under this subsection may only be brought by or on behalf of a Florida consumer.

(e) Liability for a tort, contract claim, or consumer protection claim which is unrelated to an action brought under subsection (10) or subsection (11) does not arise solely from the failure of a controller, processor, or person to comply with this section and evidence of such may only be used as the basis to prove a cause of action under this subsection.

(11) ENFORCEMENT AND IMPLEMENTATION BY THE DEPARTMENT.—

(a) Any violation of this section is an unfair and deceptive trade practice actionable under part II of chapter 501 solely by the department against a controller, processor, or

person. If the department has reason to believe that any controller, processor, or person is in violation of this section, the department, as the enforcement authority, may bring an action against such controller, processor, or person for an unfair or deceptive act or practice. For the purpose of bringing an action pursuant to this section, ss. 501.211 and 501.212 do not apply. Civil penalties may be tripled if the violation:

1. Involves a consumer who the controller, processor, or person has actual knowledge is 16 years of age or younger; or

2. Is based on paragraph (10)(a).

(b) After the department has notified a controller, processor, or person in writing of an alleged violation, the department may in its discretion grant a 45-day period to cure the alleged violation. The 45-day cure period does not apply to a violation of subparagraph (10)(a)1. The department may consider the number and frequency of violations, the substantial likelihood of injury to the public, and the safety of persons or property when determining whether to grant 45 days to cure and the issuance of a letter of guidance. If the violation is cured to the satisfaction of the department and proof of such cure is provided to the department, the department in its discretion may issue a letter of guidance. If the controller, processor, or person fails to cure the violation within 45 days, the department may bring an action against the controller, processor, or person for the alleged violation.

(c) Any action brought by the department may only be brought by or on behalf of a Florida consumer.

(d) By February 1 of each year, the department shall submit a report to the President of the Senate and the Speaker of the House of Representatives describing any actions taken by the department to enforce this section. The report shall include statistics and relevant information detailing:

1. The number of complaints received;

2. The number and type of enforcement actions taken and the outcomes of such actions;

3. The number of complaints resolved without the need for litigation; and

4. The status of the development and implementation of rules to implement this section.

(e) The department may adopt rules to implement this section, including standards for verifiable consumer requests, enforcement, data security, and authorized persons who may act on a consumer's behalf.

(12) JURISDICTION.—For purposes of bringing an action in accordance with subsections (10) and (11), any person who meets the definition of controller as defined in this section that collects, shares, or sells the personal information of Florida consumers, is considered to be both engaged in substantial and not isolated activities within this state and operating, conducting, engaging in, or carrying on a business, and doing

business in this state, and is therefore subject to the jurisdiction of the courts of this state.

(13) PREEMPTION.—This section is a matter of statewide concern and supersedes all rules, regulations, codes, ordinances, and other laws adopted by a city, county, city and county, municipality, or local agency regarding the collection, processing, sharing, or sale of consumer personal information by a controller or processor. The regulation of the collection, processing, sharing, or sale of consumer personal information by a controller or processor is preempted to the state.

Section 2. Paragraph (g) of subsection (1) of section 501.171, Florida Statutes, is amended to read:

501.171 Security of confidential personal information.—

(1) DEFINITIONS.—As used in this section, the term:

(g)1. "Personal information" means either of the following:

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

(I) A social security number;

(II) 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;

(III) A financial account number or credit 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;

(IV) Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or

(V) An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual.

(VI) An individual's biometric information as defined in s. 501.173(2).

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.

2. 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.

Section 3. This act shall take effect July 1, 2023.

COMMERCE COMMITTEE

HB 9 by Rep. McFarland
Consumer Data Privacy

AMENDMENT SUMMARY
February 10, 2022

Amendment 1 by Rep. McFarland (strike):

- Allows a controller to provide the categories of personal information collected, rather than the specific details of the information, in certain circumstances.
- Makes exceptions uniform for “right to delete,” “right to correct,” and “controller retention.”
- Adds guidance and a list of factors for courts to consider when determining the amount of damages due in a private cause of action.
- Clarifies that a processor must only turn over personal information to a controller, not all of the processor’s information.
- Clarifies throughout the bill that a length of time in days refers to calendar days.
- Increases the age that requires an opt-in for minors, to 18 years of age, from 16.
- Clarifies and makes conforming changes throughout the bill.

COMMITTEE/SUBCOMMITTEE ACTION

ADOPTED	___ (Y/N)
ADOPTED AS AMENDED	___ (Y/N)
ADOPTED W/O OBJECTION	___ (Y/N)
FAILED TO ADOPT	___ (Y/N)
WITHDRAWN	___ (Y/N)
OTHER	_____

Committee/Subcommittee hearing bill: Commerce Committee
Representative McFarland offered the following:

Amendment (with title amendment)

Remove everything after the enacting clause and insert:

Section 1. Section 501.173, Florida Statutes, is created to read:

501.173 Consumer data privacy.—

(1) APPLICABILITY.—This section does not apply to:

(a) Personal information collected and transmitted that is necessary for the sole purpose of sharing such personal information with a financial service provider solely to facilitate short term, transactional payment processing for the purchase of products or services.

(b) Personal information collected, used, retained, sold, shared, or disclosed as deidentified personal information or

aggregate consumer information.

(c) Compliance with federal, state, or local laws.

(d) Compliance with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities.

(e) Cooperation with law enforcement agencies concerning conduct or activity that the controller, processor, or third party reasonably and in good faith believes may violate federal, state, or local law.

(f) Exercising or defending legal claims.

(g) Personal information obtained through the controller's direct interactions with the consumer, if collected in accordance with the provisions of this section, that is used by the controller or the processor that the controller directly contracts with for advertising or marketing services to advertise or market products or services that are produced or offered directly by the controller. Such information may not be sold, shared, or disclosed unless otherwise authorized under this section.

(h) Personal information of a person acting in the role of a job applicant, employee, owner, director, officer, contractor, volunteer, or intern of a controller, that is collected by a controller, to the extent the personal information is collected and used solely within the context of the person's role or former role with the controller.

(i) Protected health information for purposes of the federal Health Insurance Portability and Accountability Act of 1996 and related regulations, and patient identifying information for purposes of 42 C.F.R. part 2, established pursuant to 42 U.S.C. s. 290dd-2.

(j) A covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services in 45 C.F.R. parts 160 and 164, or a program or a qualified service program as defined in 42 C.F.R. part 2, to the extent the covered entity, business associate, or program maintains personal information in the same manner as medical information or protected health information as described in paragraph (i), and as long as the covered entity, business associate, or program does not use personal information for targeted advertising with third parties and does not sell or share personal information to a third party unless such sale or sharing is covered by an exception under this section.

(k) Identifiable private information collected for purposes of research as defined in 45 C.F.R. s. 164.501 conducted in accordance with the Federal Policy for the Protection of Human Subjects for purposes of 45 C.F.R. part 46, the good clinical practice guidelines issued by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use, or the

Protection for Human Subjects for purposes of 21 C.F.R. parts 50 and 56, or personal information that is used or shared in research conducted in accordance with one or more of these standards.

(l) Information and documents created for purposes of the federal Health Care Quality Improvement Act of 1986 and related regulations, or patient safety work product for purposes of 42 C.F.R. part 3, established pursuant to 42 U.S.C. s. 299b-21 through 299b-26.

(m) Information that is deidentified in accordance with 45 C.F.R. part 164 and derived from individually identifiable health information as described in the Health Insurance Portability and Accountability Act of 1996, or identifiable personal information, consistent with the Federal Policy for the Protection of Human Subjects or the human subject protection requirements of the United States Food and Drug Administration.

(n) Information used only for public health activities and purposes as described in 45 C.F.R. s. 164.512.

(o) Personal information collected, processed, sold, or disclosed pursuant to the federal Fair Credit Reporting Act, 15 U.S.C. s. 1681 and implementing regulations.

(p) Nonpublic personal information collected, processed, sold, or disclosed pursuant to the Gramm-Leach-Bliley Act, 15 U.S.C. s. 6801 et seq., and implementing regulations.

(q) A financial institution as defined in the Gramm-Leach-

Bliley Act, 15 U.S.C. s. 6801 et seq., to the extent the financial institution maintains personal information in the same manner as nonpublic personal information as described in paragraph (p), and as long as such financial institution does not use personal information for targeted advertising with third parties and does not sell or share personal information to a third party unless such sale or sharing is covered by an exception under this section.

(r) Personal information collected, processed, sold, or disclosed pursuant to the federal Driver's Privacy Protection Act of 1994, 18 U.S.C. s. 2721 et seq.

(s) Education information covered by the Family Educational Rights and Privacy Act, 20 U.S.C. s. 1232(g) and 34 C.F.R. part 99.

(t) Information collected as part of public or peer-reviewed scientific or statistical research in the public interest and that adheres to all other applicable ethics and privacy laws, if the consumer has provided informed consent. Research with personal information must be subjected by the controller conducting the research to additional security controls that limit access to the research data to only those individuals necessary to carry out the research purpose and subsequently deidentified.

(u) Personal information disclosed for the purpose of responding to an alert of a present risk of harm to a person or

property or prosecuting those responsible for that activity.

(v) Personal information that is disclosed when a consumer uses or directs a controller to intentionally disclose information to a third party or uses the controller to intentionally interact with a third party. An intentional interaction occurs when the consumer intends to interact with the third party, by one or more deliberate interactions. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer's intent to interact with a third party.

(w) An identifier used for a consumer who has opted out of the sale or sharing of the consumer's personal information for the sole purpose of alerting processors and third parties that the consumer has opted out of the sale or sharing of the consumer's personal information.

(x) Personal information transferred by a controller to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller, provided that information is used or shared consistently with this section. If a third party materially alters how it uses or shares the personal information of a consumer in a manner that is materially inconsistent with the commitments or promises made at the time of collection, it shall provide prior notice of the new or changed practice to the consumer. The notice must be

sufficiently prominent and robust to ensure that consumers can easily exercise choices consistent with this section.

(2) DEFINITIONS.—As used in this section, the term:

(a) "Aggregate consumer information" means information that relates to a group or category of consumers, from which the identity of an individual consumer has been removed and is not reasonably capable of being directly or indirectly associated or linked with, any consumer, household, or device. The term does not include personal information that has been deidentified.

(b) "Biometric information" means an individual's physiological, biological, or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. The term includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.

(c) "Collect" means to buy, rent, gather, obtain, receive, or access any personal information pertaining to a consumer by any means. The term includes, but is not limited to, actively or passively receiving information from the consumer or by

observing the consumer's behavior or actions.

(d) "Consumer" means a natural person who resides in or is domiciled in this state, however identified, including by any unique identifier, who is acting in a personal capacity or household context. The term does not include a natural person acting on behalf of a legal entity in a commercial or employment context.

(e) "Controller" means:

1. A sole proprietorship, partnership, limited liability company, corporation, association, or legal entity that meets the following requirements:

a. Is organized or operated for the profit or financial benefit of its shareholders or owners;

b. Does business in this state;

c. Collects personal information about consumers, or is the entity on behalf of which such information is collected;

d. Determines the purposes and means of processing personal information about consumers alone or jointly with others; and

e. Satisfies at least two of the following thresholds:

(I) Has global annual gross revenues in excess of $50 million, as adjusted in January of every odd-numbered year to reflect any increase in the Consumer Price Index.

(II) Annually buys, receives, sells, or shares the personal information of 50,000 or more consumers, households,

and devices for the purpose of targeted advertising in conjunction with third parties or for a purpose that is not listed under subsection (1).

(III) Derives 50 percent or more of its global annual revenues from selling or sharing personal information about consumers.

2. Any entity that controls or is controlled by a controller. As used in this subparagraph, the term "control" means:

a. Ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a controller;

b. Control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or

c. The power to exercise a controlling influence over the management of a company.

(f) "Deidentified" means information that cannot reasonably be used to infer information about or otherwise be linked to a particular consumer, provided that the controller that possesses the information:

1. Takes reasonable measures to ensure that the information cannot be associated with a specific consumer;

2. Maintains and uses the information in deidentified form and not to attempt to reidentify the information, except that

the controller may attempt to reidentify the information solely for the purpose of determining whether its deidentification processes satisfy the requirements of this paragraph; and

3. Contractually obligates any recipients of the information to comply with all the provisions of this paragraph to avoid reidentifying such information.

(g) "Department" means the Department of Legal Affairs.

(h) "Device" means a physical object associated with a consumer or household capable of directly or indirectly connecting to the Internet.

(i) "Homepage" means the introductory page of an Internet website and any Internet webpage where personal information is collected. In the case of a mobile application, the homepage is the application's platform page or download page, a link within the application, such as the "About" or "Information" application configurations, or settings page, and any other location that allows consumers to review the notice required by subsection (7), including, but not limited to, before downloading the application.

(j) "Household" means a natural person or a group of people in this state who reside at the same address, share a common device or the same service provided by a controller, and are identified by a controller as sharing the same group account or unique identifier.

(k) "Personal information" means information that is

linked or reasonably linkable to an identified or identifiable consumer or household, including biometric information and unique identifiers to the consumer. The term does not include consumer information that is:

1. Consumer employment contact information, including a position name or title, employment qualifications, emergency contact information, business telephone number, business electronic mail address, employee benefit information, and similar information used solely in an employment context.

2. Deidentified or aggregate consumer information.

3. Publicly and lawfully available information reasonably believed to be made available to the public in a lawful manner and without legal restrictions:

a. From federal, state, or local government records.

b. By a widely distributed media source.

c. By the consumer or by someone to whom the consumer disclosed the information unless the consumer has purposely and effectively restricted the information to a certain audience on a private account.

(l) "Processing" means any operation or set of operations that are performed on personal information or on sets of personal information, whether or not by automated means.

(m) "Processor" means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or

financial benefit of its shareholders or other owners, that processes information on behalf of a controller and to which the controller discloses a consumer's personal information pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the controller, as permitted by this section.

(n) "Sell" means to sell, rent, release, disclose, disseminate, make available, transfer, or otherwise communicate orally, in writing, or by electronic or other means, a consumer's personal information by a controller to another controller or a third party for monetary or other valuable consideration.

(o) "Share" means to share, rent, release, disclose, disseminate, make available, transfer, or access a consumer's personal information for advertising or marketing. The term includes:

1. Allowing a third party to use or advertise or market to a consumer based on a consumer's personal information without disclosure of the personal information to the third party.

2. Monetary transactions, nonmonetary transactions, and transactions for other valuable consideration between a controller and a third party for advertising or marketing for the benefit of a controller.

(p) "Targeted advertising" means marketing to a consumer or displaying an advertisement to a consumer when the advertisement is selected based on personal information used to predict such consumer's preferences or interests.

(q) "Third party" means a person who is not a controller or processor.

(r) "Verifiable consumer request" means a request related to personal information that is made by a consumer, by a parent or guardian on behalf of a consumer who is a minor child, or by a person authorized by the consumer to act on the consumer's behalf, in a form that is reasonably and readily accessible to consumers and that the controller can reasonably verify to be the consumer, pursuant to rules adopted by the department.

(3) CONSUMER DATA COLLECTION REQUIREMENTS AND RESPONSIBILITIES.—

(a) A controller that collects personal information about consumers shall maintain an up-to-date online privacy policy and make such policy available from its homepage. The online privacy policy must include the following information:

1. Any Florida-specific consumer privacy rights.

2. A list of the types and categories of personal information the controller collects, sells, or shares, or has collected, sold, or shared, about consumers.

3. The consumer's right to request deletion or correction of certain personal information.

4. The consumer's right to opt-out of the sale or sharing to third parties.

(b) A controller that collects personal information shall, at or before the point of collection, inform, or direct the processor to inform, consumers of the categories of personal information to be collected and the purposes for which the categories of personal information will be used.

(c) A controller may not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section.

(d) A controller that collects a consumer's personal information shall implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure.

(e) A controller shall adopt and implement a retention schedule that prohibits the use or retention of personal information not subject to an exemption by the controller or processor after the satisfaction of the initial purpose for which such information was collected or obtained, after the expiration or termination of the contract pursuant to which the information was collected or obtained, or 3 years after the consumer's last interaction with the controller. This paragraph

does not apply to personal information reasonably used or retained to do any of the following:

1. Fulfill the terms of a written warranty or product recall conducted in accordance with federal law.

2. Provide a good or service requested by the consumer, or reasonably anticipate the request of such good or service within the context of a controller's ongoing business relationship with the consumer.

3. Detect security threats or incidents; protect against malicious, deceptive, fraudulent, unauthorized, or illegal activity or access; or prosecute those responsible for such activity or access.

4. Debug to identify and repair errors that impair existing intended functionality.

5. Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws when the controller's deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent.

6. Enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the controller or that are compatible with the context in which the consumer provided the information.

7. Comply with a legal obligation, including any state or

federal retention laws.

8. As reasonably needed to protect the controller's interests against existing disputes, legal action, or governmental investigations.

9. Assure the physical security of persons or property.

(4) CONSUMER RIGHT TO REQUEST COPY OF PERSONAL DATA COLLECTED, SOLD, OR SHARED.—

(a) A consumer has the right to request that a controller that collects, sells, or shares personal information about the consumer to disclose the following to the consumer:

1. The specific pieces of personal information that have been collected about the consumer.

2. The categories of sources from which the consumer's personal information was collected.

3. The specific pieces of personal information about the consumer that were sold or shared.

4. The third parties to which the personal information about the consumer was sold or shared.

5. The categories of personal information about the consumer that were disclosed to a processor.

(b) A controller that collects, sells, or shares personal information about a consumer shall disclose the information specified in paragraph (a) to the consumer upon receipt of a verifiable consumer request.

(c) This subsection does not require a controller to

retain, reidentify, or otherwise link any data that, in the ordinary course of business is not maintained in a manner that would be considered personal information.

(d) The controller shall deliver the information required or act on the request in this subsection to a consumer free of charge within 45 calendar days after receiving a verifiable consumer request. The response period may be extended once by 45 additional calendar days when reasonably necessary, provided the controller informs the consumer of any such extension within the initial 45-day response period and the reason for the extension. The information must be delivered in a readily usable format. A controller is not obligated to provide information to the consumer if the consumer or a person authorized to act on the consumer's behalf does not provide verification of identity or verification of authorization to act with the permission of the consumer.

(e) A controller may provide personal information to a consumer at any time, but is not required to provide personal information to a consumer more than twice in a 12-month period.

(f) This subsection does not apply to personal information relating solely to households.

(5) RIGHT TO HAVE PERSONAL INFORMATION DELETED OR CORRECTED.—

(a) A consumer has the right to request that a controller delete any personal information about the consumer which the

controller has collected from the consumer.

1. A controller that receives a verifiable consumer request to delete the consumer's personal information shall delete the consumer's personal information from its records and direct any processors to delete such information within 90 calendar days of receipt of the verifiable consumer request.

2. A controller or a processor acting pursuant to its contract with the controller may not be required to comply with a consumer's request to delete the consumer's personal information if it is reasonably necessary for the controller or processor to maintain the consumer's personal information to do any of the following:

a. Complete the transaction for which the personal information was collected.

b. Fulfill the terms of a written warranty or product recall conducted in accordance with federal law.

c. Provide a good or service requested by the consumer, or reasonably anticipate the request of such good or service within the context of a controller's ongoing business relationship with the consumer, or otherwise perform a contract between the controller and the consumer.

d. Detect security threats or incidents; protect against malicious, deceptive, fraudulent, unauthorized, or illegal activity or access; or prosecute those responsible for such activity or access.

e. Debug to identify and repair errors that impair existing intended functionality.

f. Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws when the controller's deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent.

g. Enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the controller or that are compatible with the context in which the consumer provided the information.

h. Comply with a legal obligation, including any state or federal retention laws.

i. As reasonably needed to protect the controller's interests against existing disputes, legal action, or governmental investigations.

j. Assure the physical security of persons or property.

(b) A consumer has the right to make a request to correct inaccurate personal information to a controller that maintains inaccurate personal information about the consumer. A controller that receives a verifiable consumer request to correct inaccurate personal information shall use commercially reasonable efforts to correct the inaccurate personal information as directed by the consumer and direct any

processors to correct such information within 90 calendar days after receipt of the verifiable consumer request. If a controller maintains a self-service mechanism to allow a consumer to correct certain personal information, the controller may require the consumer to correct their own personal information through such mechanism. A controller or a processor acting pursuant to its contract with the controller may not be required to comply with a consumer's request to correct the consumer's personal information if it is reasonably necessary for the controller or processor to maintain the consumer's personal information to do any of the following:

1. Complete the transaction for which the personal information was collected.

2. Fulfill the terms of a written warranty or product recall conducted in accordance with federal law.

3. Detect security threats or incidents; protect against malicious, deceptive, fraudulent, unauthorized, or illegal activity or access; or prosecute those responsible for such activity or access.

4. Debug to identify and repair errors that impair existing intended functionality.

5. Enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the controller or that are compatible with the context in which the consumer provided the information.

6. Comply with a legal obligation, including any state or federal retention laws.

7. As reasonably needed to protect the controller's interests against existing disputes, legal action, or governmental investigations.

8. Assure the physical security of persons or property.

(6) RIGHT TO OPT-OUT OF THE SALE OR SHARING OF PERSONAL INFORMATION.—

(a) A consumer has the right at any time to direct a controller not to sell or share the consumer's personal information to a third party. This right may be referred to as the right to opt-out.

(b) Notwithstanding paragraph (a), a controller may not sell or share the personal information of a minor consumer if the controller has actual knowledge that the consumer is not 18 years of age or older. However, if a consumer who is between 13 and 18 years of age, or if the parent or guardian of a consumer who is 12 years of age or younger, has affirmatively authorized the sale or sharing of such consumer's personal information, then a controller may sell or share such information in accordance with this section. A controller that willfully disregards the consumer's age is deemed to have actual knowledge of the consumer's age. A controller that complies with the verifiable parental consent requirements of the Children's Online Privacy Protection Act, 15 U.S.C. s. 6501 et seq., shall

be deemed compliant with any obligation to obtain parental consent.

(c) A controller that has received direction prohibiting the sale or sharing of the consumer's personal information is prohibited from selling or sharing the consumer's personal information beginning 48 hours after receipt of such direction, unless the consumer subsequently provides express authorization for the sale or sharing of the consumer's personal information.

(7) FORM TO OPT-OUT OF SALE OR SHARING OF PERSONAL INFORMATION.—

(a) A controller shall:

1. In a form that is reasonably accessible to consumers, provide a clear and conspicuous link on the controller's Internet homepage, entitled "Do Not Sell or Share My Personal Information," to an Internet webpage that enables a consumer, or a person authorized by the consumer, to opt-out of the sale or sharing of the consumer's personal information. A controller may not require a consumer to create an account in order to direct the controller not to sell the consumer's personal information. A controller may accept a request to opt-out received through a user-enabled global privacy control, such as a browser plug-in or privacy setting, device setting, or other mechanism, which communicates or signals the consumer's choice to opt out.

2. For consumers who opted-out of the sale or sharing of their personal information, respect the consumer's decision to

opt-out for at least 12 months before requesting that the consumer authorize the sale or sharing of the consumer's personal information.

3. Use any personal information collected from the consumer in connection with the submission of the consumer's opt-out request solely for the purposes of complying with the opt-out request.

(b) A consumer may authorize another person to opt-out of the sale or sharing of the consumer's personal information on the consumer's behalf pursuant to rules adopted by the department.

(8) ACTIONS RELATED TO CONSUMERS WHO EXERCISE PRIVACY RIGHTS.—

(a) A controller may charge a consumer who exercised any of the consumer's rights under this section a different price or rate, or provide a different level or quality of goods or services to the consumer, only if that difference is reasonably related to the value provided to the controller by the consumer's data or is related to a consumer's voluntary participation in a financial incentive program, including a bona fide loyalty, rewards, premium features, discounts, or club card program offered by the controller.

(b) A controller may offer financial incentives, including payments to consumers as compensation, for the collection, sharing, sale, or deletion of personal information if the

consumer gives the controller prior consent that clearly describes the material terms of the financial incentive program. The consent may be revoked by the consumer at any time.

(c) A controller may not use financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature.

(9) CONTRACTS AND ROLES.—

(a) Any contract or agreement between a controller and a processor must:

1. Prohibit the processor from selling, sharing, retaining, using, or disclosing the personal information for any purpose that violates this section;

2. Govern the processor's personal information processing procedures with respect to processing performed on behalf of the controller, including processing instructions, the nature and purpose of processing, the type of information subject to processing, the duration of processing, and the rights and obligations of both the controller and processor;

3. Require the processor to return or delete all personal information under the contract to the controller as requested by the controller at the end of the provision of services, unless retention of the information is required by law; and

4. Upon request of the controller, require the processor to make available to the controller all personal information in its possession under the contract or agreement.

(b) Determining whether a person is acting as a controller

or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal information is to be processed. The contract between a controller and processor must reflect their respective roles and relationships related to handling personal information. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal information remains a processor.

(c) A third party may not sell or share personal information about a consumer that has been sold or shared to the third party by a controller unless the consumer has received explicit notice from the third party and is provided an opportunity to opt-out by the third party.

(d) A processor or third party must require any subcontractor to meet the same obligations of such processor or third party with respect to personal information.

(e) A processor or third party or any subcontractor thereof who violates any of the restrictions imposed upon it under this section is liable or responsible for any failure to comply with this section.

(f) Any provision of a contract or agreement of any kind that waives or limits in any way a consumer's rights under this section, including, but not limited to, any right to a remedy or means of enforcement, is deemed contrary to public policy and is void and unenforceable. This section does not prevent a consumer

from declining to request information from a controller, declining to opt-out of a controller's sale or sharing of the consumer's personal information, or authorizing a controller to sell or share the consumer's personal information after previously opting out.

(10) CIVIL ACTIONS; PRIVATE RIGHT OF ACTION.—

(a) A Florida consumer may only bring a civil action against a controller, processor, or third party pursuant to this section for the following:

1. Failure to delete or correct the consumer's personal information pursuant to this section after receiving a verifiable consumer request or directions to delete or correct from a controller unless the controller, processor, or third party qualifies for an exception to the requirements to delete or correct under this section.

2. Continuing to sell or share the consumer's personal information after the consumer chooses to opt-out pursuant to this section.

3. Selling or sharing the personal information of the consumer age 18 or younger without obtaining consent as required by this section.

(b) A court may grant the following relief to a Florida consumer:

1. Statutory damages in an amount not less than $100 and not greater than $750 per consumer per incident or actual

damages, whichever is greater.

2. Injunctive or declaratory relief.

(c) Upon prevailing, the Florida consumer shall recover reasonable attorney fees and costs.

(d) Any action under this subsection may only be brought by or on behalf of a Florida consumer.

(e) Liability for a tort, contract claim, or consumer protection claim which is unrelated to an action brought under subsection (10) or subsection (11) does not arise solely from the failure of a controller, processor, or third party to comply with this section and evidence of such may only be used as the basis to prove a cause of action under this subsection.

(f) In assessing the amount of statutory damages, the court shall consider any one or more of the relevant circumstances presented by any of the parties to the case, including, but not limited to, the nature and seriousness of the misconduct, the number of violations, the length of time over which the misconduct occurred, and the defendant's assets, liability, and net worth.

(11) ENFORCEMENT AND IMPLEMENTATION BY THE DEPARTMENT.—

(a) Any violation of this section is an unfair and deceptive trade practice actionable under part II of chapter 501 solely by the department against a controller, processor, or person. If the department has reason to believe that any controller, processor, or third party is in violation of this

section, the department, as the enforcement authority, may bring an action against such controller, processor, or third party for an unfair or deceptive act or practice. For the purpose of bringing an action pursuant to this section, ss. 501.211 and 501.212 do not apply. Civil penalties may be tripled if the violation:

1. Involves a Florida consumer who the controller, processor, or third party has actual knowledge is 18 years of age or younger; or

2. Is based on paragraph (10)(a).

(b) After the department has notified a controller, processor, or third party in writing of an alleged violation, the department may in its discretion grant a 45-day period to cure the alleged violation. The 45-day cure period does not apply to a violation of subparagraph (10)(a)1. The department may consider the number and frequency of violations, the substantial likelihood of injury to the public, and the safety of persons or property when determining whether to grant 45 calendar days to cure and the issuance of a letter of guidance. If the violation is cured to the satisfaction of the department and proof of such cure is provided to the department, the department in its discretion may issue a letter of guidance. If the controller, processor, or third party fails to cure the violation within 45 calendar days, the department may bring an action against the controller, processor, or third party for the

alleged violation.

(c) Any action brought by the department may only be brought on behalf of a Florida consumer.

(d) By February 1 of each year, the department shall submit a report to the President of the Senate and the Speaker of the House of Representatives describing any actions taken by the department to enforce this section. The report shall include statistics and relevant information detailing:

1. The number of complaints received;

2. The number and type of enforcement actions taken and the outcomes of such actions;

3. The number of complaints resolved without the need for litigation; and

4. The status of the development and implementation of rules to implement this section.

(e) The department may adopt rules to implement this section, including standards for verifiable consumer requests, enforcement, data security, and authorized persons who may act on a consumer's behalf.

(12) JURISDICTION.—For purposes of bringing an action in accordance with subsections (10) and (11), any person who meets the definition of controller as defined in this section that collects, shares, or sells the personal information of Florida consumers, is considered to be both engaged in substantial and not isolated activities within this state and operating,

conducting, engaging in, or carrying on a business, and doing business in this state, and is therefore subject to the jurisdiction of the courts of this state.

(13) PREEMPTION.—This section is a matter of statewide concern and supersedes all rules, regulations, codes, ordinances, and other laws adopted by a city, county, city and county, municipality, or local agency regarding the collection, processing, sharing, or sale of consumer personal information by a controller or processor. The regulation of the collection, processing, sharing, or sale of consumer personal information by a controller or processor is preempted to the state.

Section 2. Paragraph (g) of subsection (1) of section 501.171, Florida Statutes, is amended to read:

501.171 Security of confidential personal information.—

(1) DEFINITIONS.—As used in this section, the term:

(g)1. "Personal information" means either of the following:

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

(I) A social security number;

(II) 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;

(III) A financial account number or credit 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;

(IV) Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or

(V) An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual.

(VI) An individual's biometric information as defined in s. 501.173(2).

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.

2. 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.

Section 3. This act shall take effect July 1, 2023.

T I T L E A M E N D M E N T

Remove everything before the enacting clause and insert:

A bill to be entitled

An act relating to consumer data privacy; creating s. 501.173, F.S.; providing applicability; providing definitions; requiring controllers that collect a consumer's personal data to disclose certain information regarding data collection and selling practices to the consumer at or before the point of collection; specifying that such information may be provided through a general privacy policy or through a notice informing the consumer that additional specific information will be provided upon a certain request; prohibiting controllers from collecting additional categories of personal information or using personal information for additional purposes without notifying the consumer; requiring controllers that collect personal information to implement reasonable security procedures and practices to protect the information; authorizing consumers to request controllers to disclose the specific personal information the controller has collected about the consumer; requiring controllers to make available two or more methods for consumers to request their personal information; requiring controllers to provide such information free

of charge within a certain timeframe and in a certain format upon receiving a verifiable consumer request; specifying requirements for third parties with respect to consumer information acquired or used; providing construction; authorizing consumers to request controllers to delete or correct personal information the controllers have collected about the consumers; providing exceptions; specifying requirements for controllers to comply with deletion or correction requests; authorizing consumers to opt out of third-party disclosure of personal information collected by a controller; prohibiting controllers from selling or disclosing the personal information of consumers younger than a certain age, except under certain circumstances; prohibiting controllers from selling or sharing a consumer's information if the consumer has opted out of such disclosure; prohibiting controllers from taking certain actions to retaliate against consumers who exercise certain rights; providing applicability; providing that a contract or agreement that waives or limits certain consumer rights is void and unenforceable; providing for civil actions and a private right of action for consumers under certain circumstances; providing civil remedies; authorizing the Department of Legal Affairs to bring an action

under the Florida Unfair or Deceptive Trade Practices Act and to adopt rules; requiring the department to submit an annual report to the Legislature; providing report requirements; providing that controllers must have a specified timeframe to cure any violations; providing jurisdiction; declaring that the act is matter of statewide concern; preempting the collection, processing, sharing, and sale of consumer personal information to the state; amending s. 501.171, F.S.; revising the definition of "personal information"; providing an effective date.

HB 631

HOUSE OF REPRESENTATIVES STAFF ANALYSIS

BILL #: HB 631 Airport Funding
SPONSOR(S): Grall
TIED BILLS: **IDEN./SIM. BILLS:** SB 780

REFERENCE	ACTION	ANALYST	STAFF DIRECTOR or BUDGET/POLICY CHIEF
1) Tourism, Infrastructure & Energy Subcommittee	17 Y, 0 N	Neuffer	Keating
2) Commerce Committee		Neuffer	Hamon

SUMMARY ANALYSIS

The Federal Aviation Administration (FAA) oversees the planning and development of airports across the nation with a focus on safety and security. In order to further its goal, the FAA provides grants through the Airport Improvement Program (AIP) for the funding of airport infrastructure projects. The FAA classifies all airports using data related to the number of passengers that board an aircraft (passenger boardings).

To qualify for AIP funding, an airport must be included in the National Plan of Integrated Airport Systems (NPIAS), a database which is published every two years. The NPIAS classifies airports by category and hub. The amount of funding through the AIP is dependent upon the classification of the airport.

The Florida Department of Transportation (DOT) provides financial assistance to airports in the areas of safety, security, preservation, capacity improvement, land acquisition, planning, and economic development through its Aviation Grant Program. The Aviation Grant Program is funded from the State Transportation Trust Fund. Unless otherwise provided in the General Appropriations Act or a substantive bill implementing it, DOT may participate, if funds are available, in the capital cost of eligible public airport and aviation development projects.

DOT may provide, when such funding is available, up to 50 percent of eligible project costs to commercial service airports. General aviation airports may receive up to 80 percent funding from DOT for eligible costs so long as the airport has no scheduled commercial service.

The bill permits DOT funding for up to 80 percent of eligible project costs for airports classified as commercial service or general aviation with fewer than 100,000 annual passenger boardings. DOT funding will continue to come from the Aviation Grant fund. Annual passenger boardings will be determined by the FAA.

The bill does not impact state or local government revenues. The bill appears to have an indeterminate impact on state and local government expenditures.

The bill has an effective date of July 1, 2022.

FULL ANALYSIS

I. SUBSTANTIVE ANALYSIS

A. EFFECT OF PROPOSED CHANGES:

Present Situation

Federal Classification and Funding of Airports

The Federal Aviation Administration (FAA) oversees the planning and development of airports across the nation with a focus on safety and security. In order to further its goal, the FAA provides grants through the Airport Improvement Program (AIP) for the funding of airport infrastructure projects.[1] Grants are available to publicly owned airports – and, in some cases, to privately owned airports – for planning and development,[2] airport noise compatibility planning,[3] and the implementation of those plans.[4]

The FAA classifies all airports using data related to the number of passengers that board an aircraft (passenger boardings).[5] The agency also considers the types of activities conducted at the airport, such as cargo service.

To qualify for AIP funding, an airport must be included in the National Plan of Integrated Airport Systems (NPIAS), a database which is published every two years.[6] The NPIAS identifies existing and proposed public-use airports that are deemed important to the national transportation system.[7] Additionally, the NPIAS classifies airports by category[8] and hub.[9] The amount of grants funded through the AIP are dependent upon the classification of the airport. Large and medium primary hubs can receive up to 75 percent of eligible costs while small primary, reliever, and general aviation airports are eligible for 90 to 95 percent of qualifying costs.[10] The table below shows the federal airport classification system.

[1] 49 U.S.C. § 48103(a).
[2] 49 U.S.C. § 47104.
[3] 49 U.S.C. § 47505(a)(2).
[4] 49 U.S.C. § 47504(c).
[5] 49 U.S.C. § 47102(15) (defining "passenger boardings" as revenue passenger boardings in the United States in the prior calendar year on an aircraft in service in air commerce).
[6] FAA Order 5090.5 s. 2.3.5, September 3, 2019.
[7] *Id.*
[8] *See* FAA, *National Plan of Integration Airport Systems* (2021-2025), September 2020 (explaining a category describes the type of service the airport currently provides to the community and is anticipated to provide at the end of the 5-year planning period).
[9] *Id.* (explaining a "hub" is defined in statute to delineate commercial service airports based on the percentage of total passenger enplanements).
[10] *See* FAA, *Overview: What is AIP?*, United States Department of Transportation, https://www.faa.gov/airports/aip/overview/#:~:text=For%20large%20and%20medium%20primary,costs%2C%20based%20on%20statutory%20requirements (last visited January 28, 2022).

Airport Classifications[11]		Hub Type: Percentage of Annual Passenger Boardings	Common Name
Commercial Service: Publicly owned airports that have at least 2,500 passenger boardings each calendar year and receive scheduled passenger service	**Primary:** Have more than 10,000 passenger boardings each year	**Large:** 1% or more	**Large Hub**
		Medium: At least 0.25% but less than 1%	**Medium Hub**
		Small: At least 0.05% but less than 0.25%	**Small Hub**
		Nonhub: More than 10,000 but less than 0.05%	**Nonhub Primary**
	Nonprimary	**Nonhub:** At least 2,500 and no more than 10,000	**Nonprimary Commercial Service**
Nonprimary (other than commercial service)		**N/A**	**Reliever**

Florida Airport Funding

The Florida Department of Transportation (DOT) is tasked with the duty, function, and responsibility of planning airport systems in the state.[12] DOT is also responsible for the creation and periodic update of the statewide aviation system plan.[13] Any proposed airport[14] must receive DOT approval for any and all site acquisitions, construction, or establishment of airport facilities. A public airport[15] is required to obtain a license from DOT prior to receiving or sending any aircraft from its location, subject to inspection upon initial application for the license and renewal. While DOT operates on a statewide level, local governments are charged with adopting, administering, and enforcing airport land use compatibility zoning regulations.[16]

DOT is charged with coordinating and assisting in the development of a viable aviation system within the state.[17] It statewide aviation system plan must be developed and periodically updated with 5-year, 10-year, and 20-year summaries for the state's needs.[18] The plans set forth by DOT must be consistent with the goals of the Florida Transportation Plan and with approved local airport master plans.[19] DOT provides financial assistance to airports in the areas of safety, security, preservation, capacity improvement, land acquisition, planning, and economic development through its Aviation Grant Program.[20] The Aviation Grant Program is funded from the State Transportation Trust Fund, which Florida's aviation industry contributes to through the state aviation tax of 4.27 cents per gallon of fuel.[21] Unless otherwise provided in the General Appropriations Act or a substantive bill implementing it, DOT may participate, if funds are available, in the capital cost of eligible *public* airport and aviation development projects.[22] Operational expenses are often not considered eligible for aviation grants.[23]

[11] *See* 42 U.S.C. § 47102.
[12] S. 332.001, F.S.
[13] S. 332.006, F.S.
[14] *See* s. 330.27(2), F.S.
[15] *See* s. 330.27(6), F.S. (defining "public airport" as an airport, publicly or privately owned, which is open for use by the public).
[16] S. 333.03, F.S.
[17] S. 332.006(1), F.S.
[18] *Id.*
[19] *Id.*
[20] *See* Florida Department of Transportation, Grant Program, available at https://www.fdot.gov/aviation/fundinginfo.shtm (last visited on December 14, 2021).
[21] S. 206.9825, F.S.
[22] S. 332.007(6), F.S. (emphasis added).
[23] The Florida Department of Transportation – Aviation Office, *Florida Aviation Project Handbook 2021-2022*, pg. 7 (2021), https://fdotwww.blob.core.windows.net/sitefinity/docs/default-source/aviation/florida-aviation-project-handbook-(2020-2021)v7b5cc93c31f25452db01244377cc65215.pdf?sfvrsn=2ee80049_12 (last visited January 28, 2022).

When federal funding is available through an AIP grant, DOT may fund up to 50 percent of the nonfederal share of eligible project costs for commercial service airports.[24] The FAA determines the types of persons or entities eligible for AIP grant funding, as well as the types of projects that may be included in a grant.[25] General aviation airports may receive up to 80 percent of master planning and eligible aviation development project costs from DOT if federal funds are not available.[26] If federal funds are available, DOT may fund up to 80 percent of the nonfederal share of such projects.[27] DOT funding of up to 80 percent is limited to those airports having no scheduled commercial service.[28] Certain strategic airport investment projects are eligible for up to 100 percent funding from DOT, whether classified as commercial service or general aviation.[29]

[30]

TYPICAL FUNDING PERCENTAGES BY AIRPORT TYPE

Commercial Service Airports*

Type of Airport	Percentage of Funding		
	FAA	FDOT	Local
Large Hub	75%	12.5%	12.5%
Medium Hub			
Small Hub	90%	5%	5%
Nonhub Primary			
Nonprimary Commercial Service			
No FAA (AIP) Funding	0%	50%	50%

General Aviation Airports*

Type of Airport	Percentage of Funding		
	FAA	FDOT	Local
General Aviation	90%	8%	2%
No FAA (AIP) Funding	0%	80%	20%

*These are typical funding percentages. There are many exceptions to both FAA and FDOT typical funding percentages.

Vero Beach Regional Airport

Vero Beach Regional airport was classified as a nonprimary commercial service, nonhub[31] airport in 2017 by the FAA.[32] In 2018, annual passenger boardings surpassed the 10,000 threshold, reclassifying the airport as a commercial service primary, nonhub airport.[33] Annual passenger boardings decreased in 2019 to slightly under 10,000, reclassifying Vero Beach Regional as a nonprimary commercial service, nonhub airport. In 2020, annual passenger boardings decreased drastically resulting in a reclassification by the FAA to a general aviation airport.[34]

---

[24] S. 332.007(6)(a), F.S.; AIP funding is available to sponsors, which can include airports, public agencies not owning or leasing a public-use airport, metropolitan and state planning agencies.
[25] *See* United States Department of Transportation, Order 5100.38D, Change 1, February 26, 2019 (explaining a recipient of an AIP grant is normally called a sponsor).
[26] S. 332.007(6)(c), F.S.
[27] *Id.*
[28] Florida Department of Transportation, supra note 22.
[29] *See* s. 332.007(9), F.S. (providing for project criteria qualifying for 100 percent DOT funding).
[30] The Florida Department of Transportation – Aviation Office, *Florida Aviation Project Handbook 2021-2022*, pg. 7 (2021), https://fdotwww.blob.core.windows.net/sitefinity/docs/default-source/aviation/florida-aviation-project-handbook-(2020-2021)v7b5cc93c31f25452db01244377cc65215.pdf?sfvrsn=2ee80049_12 (last visited January 28, 2022).
[31] This classification was assigned as the airport had scheduled passenger service and 9,110 enplanements.
[32] *See* FAA, *Calendar Year 2019 Final Revenue Enplanements at All Airports*, September 25, 2020.
[33] This classification was assigned as the airport had scheduled passenger service and more 10,314 enplanements during the year, but less than 0.05 percent of the annual U.S. commercial enplanements.; *see* FAA, *Calendar Year 2018 Final Revenue Enplanements at All Airports*, December 20, 2019.
[34] *See* FAA, *Calendar Year 2020 Enplanements at U.S. Airports, by State*, November 8, 2021 (showing a 69.64% decrease in enplanements from 2019 to 2020).

In December of 2015, Elite Airways began direct, non-stop service from Vero Beach to Newark and other destinations. City officials did not expect the commercial service to grow at the rate it did, surpassing the 10,000 annual enplanement cap set by the FAA for non-primary, nonhub airports.[35] As a result of the reclassification, Vero Beach Regional stood to lose funding from DOT. Instead of receiving up to 80 percent for eligible projects when classified as a general aviation airport, it would only be eligible for up to 50 percent as a commercial service airport.[36]

Effect of the Bill

The bill permits DOT funding for up to 80 percent of eligible project costs for airports classified as commercial service or general aviation with fewer than 100,000 annual passenger boardings. DOT funding will continue to come from the Aviation Grant fund. Annual passenger boardings will be determined by the FAA.

B. SECTION DIRECTORY:

Section 1 Amends s. 332.007, F.S.; related to FDOT funding eligibility.

Section 2 Provides an effective date.

II. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT

A. FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues:

   None.

2. Expenditures:

   Indeterminate.[37] *See* Fiscal Comments.

B. FISCAL IMPACT ON LOCAL GOVERNMENTS:

1. Revenues:

   None.

2. Expenditures:

   Indeterminate.[38] *See* Fiscal Comments.

C. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR:

None.

D. FISCAL COMMENTS:

[35] Nicole Rodriguez, *Vero City Council 'Blindsided' by Airport Funding Problem*, VeroNews.com (January 23, 2020), http://veronews.com/2020/01/23/vero-city-council-blindsided-by-airport-funding-problem/ (last visited January 27, 2022).
[36] *See* FAA, *Passenger Boarding (Enplanement) and All-Cargo Data for U.S. Airports – Previous Years Airports*, https://www.faa.gov/airports/planning_capacity/passenger_allcargo_stats/passenger/previous_years/ (last visited January 31, 2022) (providing data that Fort Lauderdale Executive airport also appears to be trending upward in annual passenger boardings. In 2018, annual boardings increased 141 percent from the previous year. In 2019, annual passenger boardings increased 523 percent to reach 7,386).
[37] *See* Florida Department of Transportation, Agency Analysis of 2021 House Bill 631, p. 5-6 (November 05, 2021).
[38] *Id.*

The bill expands the number of airports qualifying for a larger percentage of DOT funding for eligible projects. This change could impact the opportunity of these airports to engage in eligible types of projects as the local match requirement is decreased. The cost is shifted to the state, and while the match required is indeterminate, all costs are still limited to available aviation project funding within DOT's adopted Work Program.

III. COMMENTS

A. CONSTITUTIONAL ISSUES:

1. Applicability of Municipality/County Mandates Provision:

   Not applicable. The bill does not appear to require counties or municipalities to spend funds or take action requiring the expenditure of funds; reduce the authority that counties or municipalities have to raise revenue in the aggregate; or reduce the percentage of sales tax shared with counties or municipalities

2. Other:

   None.

B. RULE-MAKING AUTHORITY:

The bill requires neither rulemaking nor does it provide a grant of rulemaking authority.

C. DRAFTING ISSUES OR OTHER COMMENTS:

None.

IV. AMENDMENTS/COMMITTEE SUBSTITUTE CHANGES

Not applicable.

A bill to be entitled

An act relating to airport funding; amending s. 332.007, F.S.; revising the types of airports eligible for specified funding of master planning and eligible aviation development projects by the Department of Transportation; providing an effective date.

Be It Enacted by the Legislature of the State of Florida:

Section 1. Paragraph (c) of subsection (6) of section 332.007, Florida Statutes, is amended to read:

332.007 Administration and financing of aviation and airport programs and projects; state plan.—

(6) Subject to the availability of appropriated funds, the department may participate in the capital cost of eligible public airport and aviation development projects in accordance with the following rates, unless otherwise provided in the General Appropriations Act or the substantive bill implementing the General Appropriations Act:

(c) When federal funds are not available, the department may fund up to 80 percent of master planning and eligible aviation development projects at publicly owned, publicly operated airports. If federal funds are available, the department may fund up to 80 percent of the nonfederal share of such projects. Such funding is limited to general aviation

CODING: Words stricken are deletions; words underlined are additions.

airports, or commercial service airports that have fewer than 100,000 passenger boardings per year as determined by the Federal Aviation Administration ~~airports that have no scheduled commercial service~~.

Section 2. This act shall take effect July 1, 2022.

CODING: Words ~~stricken~~ are deletions; words underlined are additions.

HB 695

HOUSE OF REPRESENTATIVES STAFF ANALYSIS

BILL #: HB 695 Property Insurer Reimbursements
SPONSOR(S): Stevenson
TIED BILLS: **IDEN./SIM. BILLS:** SB 1058

REFERENCE	ACTION	ANALYST	STAFF DIRECTOR or BUDGET/POLICY CHIEF
1) Insurance & Banking Subcommittee	15 Y, 0 N	Fortenberry	Luczynski
2) Appropriations Committee	24 Y, 0 N	Lee	Pridgeon
3) Commerce Committee		Fortenberry	Luczynski

SUMMARY ANALYSIS

The Florida Hurricane Catastrophe Fund (FHCF) is a tax-exempt trust fund created by the Legislature in 1993 as a form of reinsurance for residential property catastrophic hurricane losses. As a condition of transacting insurance business in the state, residential property insurers are required to enter contracts with the State Board of Administration (SBA) to purchase reimbursement coverage (reinsurance) on their residential property exposure.

As part of its regulation, the Office of Insurance Regulation (OIR) monitors the solvency of insurers to protect policyholders against the risk that insurers will not be able to meet their financial responsibilities. If an insurer is in an unsound financial condition, OIR may refer that insurer to the Department of Financial Services for the filing of a delinquency proceeding in circuit court, which may result in the liquidation of the insurer. If Citizens Property Insurance Corporation (Citizens) assumes policies from such liquidated insurer, Citizens may obtain coverage from the FHCF for these policies under its reimbursement contract with the SBA or by accepting an assignment of the liquidated insurer's reimbursement contract with the SBA. However, current law does not address the transfer of FHCF coverage to Citizens if it assumes policies from an authorized insurer that is in an unsound financial condition, but is not the subject of a delinquency proceeding, or the transfer of FHCF coverage if an authorized private insurer assumes policies from an unsound insurer.

The bill defines "unsound insurer" as an insurer that OIR has determined to be in unsound condition as defined in s. 624.80(2), F.S., or an insurer that has been placed into receivership under ch. 631, F.S. The bill allows any authorized insurer to receive the transfer of FHCF coverage along with policies that it assumes from an unsound insurer, subject to an agreement with the SBA. The bill extends to authorized insurers the requirements that exist when Citizens assumes policies from unsound insurers and wishes to obtain coverage from the FHCF for those policies and establishes additional requirements for both authorized insurers and Citizens. The bill replaces the statutory phrase "placed in liquidation" with the defined term "unsound insurer" so that FHCF coverage can be transferred to Citizens or an authorized insurer with policies that Citizens or such authorized insurer assumes from an unsound insurer or a liquidated insurer.

The bill establishes that if a covered event has occurred before the effective date of the transfer of the policies to the authorized insurer or Citizens, the authorized insurer or Citizens may only obtain coverage from the FHCF subject to an assignment of the remaining term of the unsound insurer's FHCF contract.

The bill has no impact on state or local government revenues or expenditures and no direct economic impact on the private sector.

The bill has an effective date of July 1, 2022.

FULL ANALYSIS

I. SUBSTANTIVE ANALYSIS

A. EFFECT OF PROPOSED CHANGES:

Background

Florida Hurricane Catastrophe Fund

The Florida Hurricane Catastrophe Fund (FHCF) is a tax-exempt trust fund created by the Legislature in 1993 as a form of reinsurance for residential property catastrophic hurricane losses.[1] The purpose of the FHCF is to protect and advance the state's interest in maintaining insurance capacity in Florida by providing reimbursements to insurers for a portion of their catastrophic losses.[2] The FHCF provides insurers a source of reinsurance that is stable and generally less expensive than private reinsurance.

The FHCF is administered by the State Board of Administration (SBA) and reimburses property insurers for a selected percentage of hurricane losses to residential property when those losses exceed the insurer's retention (deductible).[3] The FHCF reimburses participating insurers for losses under covered policies, subject to limitations.[4] A covered policy is defined as "any insurance policy covering residential property" in Florida, including, but not limited to the following types of policies:

- homeowner
- mobile home owner
- farm owner
- condominium association
- condominium unit owner
- tenant
- apartment building policy
- any other policy covering a residential structure or its contents.[5]

Covered policies may be issued by any authorized insurer,[6] a commercial self-insurance fund holding a certificate of authority issued by the Office of Insurance Regulation (OIR), the Citizens Property Insurance Corporation (Citizens), and any joint underwriting association or similar legal entity.[7]

As a condition of transacting insurance business in the state, residential property insurers are required to enter contracts with the SBA to purchase reimbursement coverage (reinsurance) on their residential property exposure.[8] Pursuant its contract with the SBA, each insurer must pay an actuarially-indicated annual premium for the reimbursement.[9] The actuarial basis for the premium includes an analysis of hurricane loss projection models found acceptable by the Florida Commission on Hurricane Loss Projection Methodology, which is also part of the SBA.

Insurer Financial Condition

[1] *See* s. 215.555, F.S.
[2] *See id.*
[3] *Id.* Retention is defined as the amount of losses below which an insurer is not entitled to reimbursement from the FHCF. It is calculated for each insurer based upon that insurer's proportionate share of overall premiums charged by the FHCF. *See* s. 215.555(2)(e), F.S.
[4] S. 215.555(2)(d), F.S.
[5] S. 215.555(2)(c), F.S.
[6] Authorized insurers are those insurers that have obtained a certificate of authority from OIR to transact insurance business in Florida. S. 624.09(1), F.S.
[7] S. 215.555(2)(c), F.S.
[8] S. 215.555(4), F.S.
[9] S. 215.555(5)(a), F.S.

As part of its regulation, OIR monitors the solvency of insurers to protect policyholders against the risk that insurers will not be able to meet their financial responsibilities. OIR considers an insurer to be in an unsound financial condition if:

- the insurer's required surplus, capital, or capital stock is impaired to an extent prohibited by law;
- the insurer continues to write new business when it has not maintained the required surplus or capital;
- the insurer attempted to dissolve or liquidate without making provisions for liabilities arising from insurance policies that it issued; or
- the insurer meets one or more of the grounds in s. 631.051, F.S., for appointment of the Department of Financial Services (DFS) as receiver.[10]

Federal law specifies that insurers cannot file for bankruptcy.[11] Instead, insolvent insurers are either rehabilitated or liquidated by the state. In Florida, the Division of Rehabilitation and Liquidation of DFS is responsible for rehabilitating or liquidating insurance companies.[12]

Chapter 631, F.S., relating to insurers insolvency and guaranty payments, governs the receivership process. This process involves the initiation of a delinquency proceeding in circuit court and the placement of in insurer under the control of DFS as the receiver.[13] Depending on the insurer's circumstances, the delinquency proceeding may result in an order of rehabilitation or liquidation.[14]

Assumption of Residential Property Insurance Policies by Citizens

Citizens is a state-created, not-for-profit, tax-exempt government entity that is an integral part of the state, whose public purpose is to provide property insurance to those unable to find affordable coverage in the private market from an authorized insurer.[15] Unlike private insurers, Citizens is not required to hold a certificate of authority from OIR.[16]

A significant portion of Citizens' total policy count consists of residential property insurance policies. These policies include homeowners, mobile homeowners, dwelling fire, tenants, condominium unit owners, and some other similar policies. Pursuant to its enabling statute, s. 627.351(6), F.S., Citizens must enter into a reimbursement contract with the SBA for coverage from the FHCF for its residential property insurance policies.[17] While private carriers may select from various coverage levels available from the FHCF, Citizens is statutorily required to purchase the highest available level of coverage from the FHCF.[18]

Currently, if an insurer is placed in liquidation under ch. 631, F.S., and Citizens assumes policies from such liquidated insurer, Citizens may obtain coverage from the FHCF for these policies under its reimbursement contract with the SBA or by accepting an assignment of the liquidated insurer's reimbursement contract with the SBA.[19] The assignment of the contract must be provided for in the liquidation order or otherwise determined by the court as part of the delinquency proceedings involving

---

[10] S. 624.80(2), F.S.

[11] The Bankruptcy Code expressly provides that "a domestic insurance company" may not be the subject of federal bankruptcy proceeding. 11 U.S.C. 109(b)(2). The exclusion of insurers from the federal bankruptcy process is consistent with federal policy generally allowing states to regulate insurance. *See* 15 U.S.C. ss. 1011-1012.

[12] Typically, insurers are put into liquidation when the company is insolvent, but put into rehabilitation for various other reasons, including an unsound financial condition. The goal of rehabilitation is to return the insurer to a sound financial condition. The goal of liquidation, however, is to dissolve the insurer. *See* s. 631.051, F.S., for the grounds for rehabilitation and s. 631.061, F.S., for the grounds for liquidation.

[13] S. 631.031, F.S.

[14] *See* ss. 631.101 and 631.111, F.S.

[15] S. 627.351(6)(a)1., F.S.

[16] Citizens, *Management Discussion and Analysis for 2017*, https://www.citizensfla.com/documents/20702/6867558/20180411+04E+MDA+2017.pdf/4584208b-1d87-4add-9a11-55e818fe0046?t=1523029712990 (last visited Jan. 10, 2021).

[17] *Id.*

[18] *Id.*

[19] State Board of Administration, Agency Analysis of 2022 Senate Bill 1058, p. 1 (Jan. 6, 2022). 2022 Senate Bill 1058 is identical to this bill. *See also* s. 215.555(5)(e), F.S.

the liquidated insurer.[20] The law does not address the transfer of FHCF coverage to Citizens if it assumes policies from an authorized insurer that is in an unsound financial condition (unsound insurer), but is not the subject of a delinquency proceeding.

Assumption of Residential Property Insurance Policies by Authorized Insurers

Under certain circumstances, OIR may approve the assumption of policies by an authorized insurer (assuming insurer) from an unsound insurer or an insurer placed in receivership. However, current law does not provide for the assignment to the assuming insurer of the FHCF coverage that the unsound insurer or the insurer placed in receivership has on its policies.

Effect of the Bill

The bill defines "unsound insurer" as an insurer that OIR has determined to be in unsound condition as defined in s. 624.80(2), F.S., or an insurer that has been placed into receivership under ch. 631, F.S.

The bill allows any authorized insurer to receive the transfer of FHCF coverage along with policies that it assumes from an unsound insurer, subject to an agreement with the SBA. The bill extends to authorized insurers the requirements that exist when Citizens assumes policies from unsound insurers and wishes to obtain coverage from the FHCF for those policies, and also establishes additional requirements for both authorized insurers and Citizens.

The bill replaces the statutory phrase "placed in liquidation" with the defined term "unsound insurer" so that FHCF coverage can be transferred to Citizens or an authorized insurer with policies that Citizens or such authorized insurer assumes from an unsound insurer or a liquidated insurer.

The bill establishes that if a covered event has occurred before the effective date of the transfer of the policies to the authorized insurer or Citizens, the authorized insurer or Citizens may only obtain coverage from the FHCF subject to an assignment of the remaining term of the unsound insurer's FHCF contract.

The bill removes language regarding assignments that becomes obsolete if assignment is no longer limited to policies from insurers that have been placed in liquidation under ch. 631, F.S. Finally, the bill provides that the new language regarding assignment of policies from an unsound insurer does not limit the FHCF's right to receive premium due under the contract between an unsound insurer and the FHCF.

B. SECTION DIRECTORY:

Section 1. Amends s. 215.555, F.S., relating to Florida Hurricane Catastrophe Fund.

Section 2. Provides an effective date of July 1, 2022.

II. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT

A. FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues:

None.

2. Expenditures:

None.

B. FISCAL IMPACT ON LOCAL GOVERNMENTS:

[20] S. 215.555(5)(e), F.S.

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. The bill does not appear to affect county or municipal governments.

2. Other:

   None.

B. RULE-MAKING AUTHORITY:

The bill neither authorizes nor requires administrative rulemaking.

C. DRAFTING ISSUES OR OTHER COMMENTS:

None.

IV. AMENDMENTS/COMMITTEE SUBSTITUTE CHANGES

A bill to be entitled

An act relating to property insurer reimbursements; amending s. 215.555, F.S.; defining the term "unsound insurer"; revising requirements for coverage under the Florida Hurricane Catastrophe Fund of certain policies assumed by authorized insurers or the Citizens Property Insurance Corporation; providing construction; providing an effective date.

Be It Enacted by the Legislature of the State of Florida:

Section 1. Paragraph (e) of subsection (5) of section 215.555, Florida Statutes, is amended, and paragraph (p) is added to subsection (2) of that section, to read:

215.555 Florida Hurricane Catastrophe Fund.—

(2) DEFINITIONS.—As used in this section:

(p) "Unsound insurer" means an insurer determined by the Office of Insurance Regulation to be in unsound condition as defined in s. 624.80(2) or an insurer placed in receivership under chapter 631.

(5) REIMBURSEMENT PREMIUMS.—

(e)1. If an authorized insurer or the Citizens Property Insurance Corporation assumes or otherwise provides coverage for policies of an unsound insurer ~~placed in liquidation under chapter 631 pursuant to s. 627.351(6)~~, the authorized insurer or

CODING: Words ~~stricken~~ are deletions; words underlined are additions.

the Citizens Property Insurance Corporation may, pursuant to conditions mutually agreed to between the authorized insurer or the Citizens Property Insurance Corporation and the State Board of Administration, seek to obtain coverage for such policies under its contract with the fund or accept an assignment of the unsound ~~liquidated~~ insurer's contract with the fund. However, if a covered event has occurred before the effective date of the transfer of the policies, the authorized insurer or the Citizens Property Insurance Corporation may obtain coverage for such policies only through an assignment as provided in subparagraph 3.

2. If an authorized insurer or the Citizens Property Insurance Corporation assumes policies from an unsound insurer and elects to cover these policies under its ~~the corporation's~~ contract with the fund, it shall notify the board of its insured values with respect to such policies within a specified time mutually agreed to between the authorized insurer or the Citizens Property Insurance Corporation and the board~~,~~ after such assumption ~~or other coverage transaction~~, and the fund shall treat such policies as having been in effect as of June 30 of that year.

3. If an authorized insurer or the Citizens Property Insurance Corporation accepts ~~In the event of~~ an assignment of an unsound insurer's contract, the fund shall apply the unsound insurer's ~~that~~ contract to such policies and treat the

CODING: Words ~~stricken~~ are deletions; words underlined are additions.

authorized insurer or the Citizens Property Insurance Corporation as if it ~~the corporation~~ were the unsound ~~liquidated~~ insurer for the remaining term of the contract, with ~~and the corporation shall have~~ all rights and duties of the unsound ~~liquidated~~ insurer beginning on the date it provides coverage for such policies. This subparagraph may not be construed to limit the fund's right to receive the premium due under the unsound insurer's contract~~, but the corporation is not subject to any preexisting rights, liabilities, or duties of the liquidated insurer. The assignment, including any unresolved issues between the liquidated insurer and Citizens Property Insurance Corporation under the contract, shall be provided for in the liquidation order or otherwise determined by the court. However, if a covered event occurs before the effective date of the assignment, the corporation may not obtain coverage for such policies under its contract with the fund and shall accept an assignment of the liquidated insurer's contract as provided in this paragraph~~.

Section 2. This act shall take effect July 1, 2022.

CODING: Words ~~stricken~~ are deletions; words underlined are additions.

HOUSE OF REPRESENTATIVES STAFF ANALYSIS

BILL #: HB 1565 Pub. Rec./Consumer Data Privacy
SPONSOR(S): McFarland
TIED BILLS: HB 9 **IDEN./SIM. BILLS:**

REFERENCE	ACTION	ANALYST	STAFF DIRECTOR or BUDGET/POLICY CHIEF
1) Commerce Committee		Wright	Hamon
2) Judiciary Committee			

SUMMARY ANALYSIS

As technologies that capture and analyze data proliferate, so, too, do businesses' abilities to contextualize consumer data. Businesses use it for a range of purposes. The European Union, California, and a few other states have enacted data privacy regulations to protect consumers' personal information and give consumers more control over how their information is used.

HB 9, to which this bill is linked, gives certain consumer rights related to personal information, including:

- The right to access personal information collected about them;
- The right to delete or correct their personal information; and
- The right to opt-out of the sale or sharing of their personal information to third parties.

The Department of Legal Affairs (DLA), upon belief that any controller, processor, or other person is in violation of HB 9's provisions, may bring an action under the Florida Unfair or Deceptive Trade Practices Act against a controller, processor, or other person.

This bill, which is linked to the passage of HB 9, provides that all information received by DLA pursuant to a notification or investigation by DLA or a law enforcement agency of a violation is confidential and exempt from public record requirements. The bill provides that the information may be released during an active investigation:

- In the furtherance of official duties and responsibilities;
- For print, publication, or broadcast to notify the public of a data breach; or
- To another governmental entity in the furtherance of its official duties and responsibilities.

Once an investigation is completed, the following information will remain confidential and exempt:

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

The bill provides that the public record exemption is subject to the Open Government Sunset Review Act and will repeal on October 2, 2027, unless the Legislature reviews and reenacts the exemption by that date.

Article I, s. 24(c) of the Florida Constitution requires a two-thirds vote of the members present and voting for final passage of a newly created or expanded public record or public meeting exemption. The bill creates a public record exemption; thus, it requires a two-thirds vote for final passage.

FULL ANALYSIS

I. SUBSTANTIVE ANALYSIS

A. EFFECT OF PROPOSED CHANGES:

Public Records

Article I, s. 24(a) of the State Constitution sets forth the state's public policy regarding access to government records. This section guarantees every person a right to inspect or copy any public record of the legislative, executive, and judicial branches of government. The Legislature, however, may provide by general law for the exemption of records from the requirements of Article I, section 24(a).[1] The general law must state with specificity the public necessity justifying the exemption[2] and must be no more broad than necessary to accomplish its purpose.[3]

Public policy regarding access to government records is addressed further in the Florida Statutes. Section 119.07(1), F.S., guarantees every person a right to inspect and copy any state, county, or municipal record, unless the record is exempt. Furthermore, the Open Government Sunset Review Act[4] 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.[5]

The Open Government Sunset Review Act requires the automatic repeal of a newly created exemption on October 2nd of the fifth year after creation or substantial amendment, unless the Legislature reenacts the exemption.[6]

Consumer Data Privacy

As technologies that capture and analyze data proliferate, so, too, do businesses' abilities to contextualize consumer data. Businesses use it for a range of purposes, including better understanding day-to-day operations, making more informed business decisions and learning about their customers.[7]

The European Union, several other countries, California, and a few other states have enacted data privacy regulations to protect such data and give consumers more control over how their information is used. Florida does not have a broad data privacy law, but there is a law which governs what actions must be taken by certain government and business entities in the event of a data breach of personal information.[8]

Department of Legal Affairs

The Office of the Attorney General, also known as the Department of Legal Affairs (DLA), provides a wide variety of legal services, including defending the state in civil litigation cases, representing the

[1] Art. I, s. 24(c), FLA. CONST.
[2] This portion of a public record exemption is commonly referred to as a "public necessity statement."
[3] Art. I, s. 24(c), FLA. CONST.
[4] Section 119.15, F.S.
[5] Section 119.15(6)(b), F.S.
[6] Section 119.15(3), F.S.
[7] Max Freedman, How Businesses Are Collecting Data (And What They're Doing With It), Business News Daily (Jun. 17, 2020) https://www.businessnewsdaily.com/10625-businesses-collecting-data.html.
[8] S. 501.171, F.S.

people of Florida in criminal appeals in state and federal courts, protecting rights of children, consumers, and victims through its various protection programs, and investigating and litigating against businesses that seek to limit competition and defraud taxpayers.[9]

HB 9

HB 9, to which this bill is linked, gives certain consumer rights related to personal information, including:

- The right to access personal information collected on them by a controller;
- The right to delete or correct their personal information; and
- The right to opt-out of the sale or sharing of their personal information to third parties.

A "controller" is a for profit entity that does business in Florida, collects and controls personal information, and satisfies two or more of the following thresholds:

- Has global annual gross revenues in excess of $50 million, as adjusted in January of every odd-numbered year to reflect any increase in the Consumer Price Index.
- Annually buys, receives, sells, or shares the personal information of 50,000 or more consumers, households, or devices for targeted advertising in conjunction with third parties or that is not covered by an exception.
- Derives 50 percent or more of its global annual revenues from selling or sharing personal information about consumers.

Under the bill, personal information is information that identifies, relates to, or describes a particular consumer or household, or is reasonably capable of being directly or indirectly associated or linked with, a particular consumer or household. The term does not include public information from government records, certain employment information, or deidentified or aggregate consumer information.

The bill proscribes certain operational requirements on controllers with respect to collecting, selling, or sharing personal information with processors or third parties.

DLA, upon belief that any controller, processor, or other person or entity is in violation of the consumer data requirement provisions, may bring an action under the Florida Unfair or Deceptive Trade Practices Act against a controller, processor, or other person.

Effect of the Bill

The bill creates a public record exemption for all information received by DLA pursuant to a notification or investigation by DLA or a law enforcement agency of a violation of certain statutory requirements. Such information is made confidential and exempt[10] from public record requirements.

During an active investigation, information made confidential and exempt may be disclosed by DLA:

- In the furtherance of its official duties and responsibilities;
- For print, publication, or broadcast if DLA determines that such release would assist in notifying the public or locating or identifying a person that DLA believes to be a victim of a data breach or improper use or disposal of customer records, except that information made confidential and exempt after an investigation may not be released in this manner; or
- To another governmental entity in the furtherance of its official duties and responsibilities.

[9] OPPAGA, Office of the Attorney General (Department of Legal Affairs), https://oppaga.fl.gov/ProgramSummary/ProgramDetail?programNumber=1026 (last visited Feb. 6, 2022).

[10] There is a difference between records the Legislature designates 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. Sch. Bd. of Seminole*, 874 So.2d 48, 53 (Fla. 5th DCA 2004), *review denied* 892 So.2d 1015 (Fla. 2004); *City of Rivera Beach v. Barfield*, 642 So.2d 1135 (Fla. 4th DCA 1994); *Williams v. City of Minneola*, 575 So.2d 683, 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* Op. Att'y Gen. Fla. (1985).

Once an investigation is completed or once an investigation ceases to be active, the following information received by DLA will remain confidential and exempt:

- All information to which another public records exemption applies;
- Personal information;
- A computer forensic report;
- Information that would otherwise reveal weaknesses in a controller's, processor's, or other person's data security; and
- Information that would otherwise disclose a controller's, processor's, or other person's proprietary information.

The term "proprietary information" means information that:

- Is owned or controlled by the controller, processor, or other person;
- Is intended to be private and is treated by the controller, processor, or other person as private because disclosure would harm the controller, processor, or other person or its business operations;
- Has not been disclosed except as required by law or a private agreement that provides that the information will not be released to the public;
- Is not publicly available or otherwise readily ascertainable through proper means from another source in the same configuration as received by DLA; and
- Includes trade secrets and competitive interests.

The bill provides a public necessity statement as required by article I, section 24(c) of the Florida Constitution. The public necessity statement provides that, if released, information received by DLA pursuant to an investigation by DLA or a law enforcement agency could:

- Frustrate or thwart the investigation and impair the ability of DLA to perform assigned functions;
- Undo a specific statutory exemption protecting the information;
- Be used for the purpose of identity theft;
- Result in the identification of vulnerabilities; and
- Result in economic harm.

The bill provides that the public record exemption is subject to the Open Government Sunset Review Act and will repeal on October 2, 2027, unless the Legislature reviews and reenacts the exemption by that date.

The bill will become effective on the same date that HB 9 or similar legislation takes effect, if such legislation is adopted in the same legislative session or an extension thereof and becomes a law.

B. SECTION DIRECTORY:

Section 1: Creates a public records exemption for investigations related to s. 501.173, F.S.
Section 2: Provides a public necessity statement as required by the Florida Constitution.
Section 3: Provides an effective date of the same date that HB 9 or similar legislation takes effect, if such legislation is adopted in the same legislative session or an extension thereof and becomes law.

II. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT

A. FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues:

   None.

2. Expenditures:

   See Fiscal Comments.

B. FISCAL IMPACT ON LOCAL GOVERNMENTS:

1. Revenues:

None.

2. Expenditures:

None.

C. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR:

None.

D. FISCAL COMMENTS:

The bill may have a minimal fiscal impact on DLA because agency staff responsible for complying with public records requests may require training related to the creation of the public records exemption. DLA could incur costs associated with redacting the exempt information prior to releasing a record. The costs, however, would be absorbed by existing resources, as they are part of the day-to-day responsibilities of agencies.

III. COMMENTS

A. CONSTITUTIONAL ISSUES:

1. Applicability of Municipality/County Mandates Provision:

Not applicable. The bill does not appear to require counties or municipalities to take an action requiring the expenditure of funds, reduce the authority that counties or municipalities have to raise revenue in the aggregate, nor reduce the percentage of state tax shared with counties or municipalities.

2. Other:

Vote Requirement

Article I, section 24(c) of the Florida Constitution requires a two-thirds vote of the members present and voting for final passage of a newly created or expanded public record or public meeting exemption. The bill creates a public record exemption; thus, it requires a two-thirds vote for final passage.

Public Necessity Statement

Article I, section 24(c) of the Florida Constitution requires a public necessity statement for a newly created or expanded public record or public meeting exemption. The bill creates a public record exemption; thus, it includes a public necessity statement.

Breadth of Exemption

Article 1, section 24(c) of the Florida Constitution requires a newly created or expanded public record or public meeting exemption to be no broader than necessary to accomplish the stated purpose of the law. The bill creates a public records exemption for sensitive investigative materials and personal information, which does not appear to be broader than necessary to accomplish its purpose.

B. RULE-MAKING AUTHORITY:

None.

C. DRAFTING ISSUES OR OTHER COMMENTS:

None.

IV. AMENDMENTS/COMMITTEE SUBSTITUTE CHANGES

A bill to be entitled

An act relating to public records; amending s. 501.173, F.S.; providing an exemption from public records requirements for information relating to investigations by the Department of Legal Affairs and law enforcement agencies of certain data privacy violations; providing for future legislative review and repeal of the exemption; providing a statement of public necessity; providing a contingent effective date.

Be It Enacted by the Legislature of the State of Florida:

Section 1. Subsection (14) is added to section 501.173, Florida Statutes, as created by HB 9, 2022 Regular Session, to read:

501.173 Consumer data privacy.—

(14) PUBLIC RECORDS EXEMPTION.—

(a) All information received by the department pursuant to a notification of a violation under this section, or received by the department pursuant to an investigation by the department or a law enforcement agency of a violation of this section, is confidential and exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution, until such time as the investigation is completed or ceases to be active. This exemption shall be

CODING: Words stricken are deletions; words underlined are additions.

construed in conformity with s. 119.071(2)(c).

(b) During an active investigation, information made confidential and exempt pursuant to paragraph (a) may be disclosed by the department:

1. In the furtherance of its official duties and responsibilities;

2. 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 use or disposal of customer records, except that information made confidential and exempt by paragraph (c) may not be released pursuant to this subparagraph; or

3. To another governmental entity in the furtherance of its official duties and responsibilities.

(c) Upon completion of an investigation or once an investigation ceases to be active, the following information received by the department shall remain confidential and exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution:

1. All information to which another public records exemption applies.

2. Personal information.

3. A computer forensic report.

4. Information that would otherwise reveal weaknesses in

the data security of a controller, processor, or person.

5. Information that would disclose the proprietary information of a controller, processor, or person.

(d) For purposes of this subsection, the term "proprietary information" means information that:

1. Is owned or controlled by the controller, processor, or person.

2. Is intended to be private and is treated by the controller, processor, or person as private because disclosure would harm the controller, processor, or person or its business operations.

3. Has not been disclosed except as required by law or a private agreement that provides that the information will not be released to the public.

4. Is not publicly available or otherwise readily ascertainable through proper means from another source in the same configuration as received by the department.

5. Includes:

a. Trade secrets as defined in s. 688.002.

b. Competitive interests, the disclosure of which would impair the competitive advantage of the controller, processor, or person who is the subject of the information.

(e) This subsection is subject to the Open Government Sunset Review Act in accordance with s. 119.15 and shall stand repealed on October 2, 2027, unless reviewed and saved from

repeal through reenactment by the Legislature.

Section 2. The Legislature finds that it is a public necessity that all information received by the Department of Legal Affairs pursuant to a notification of a violation of s. 501.173, Florida Statutes, or received by the department pursuant to an investigation by the department or a law enforcement agency of a violation of s. 501.173, Florida Statutes, be made confidential and exempt from s. 119.07(1), Florida Statutes, and s. 24(a), Article I of the State Constitution for the following reasons:

(1) A notification of a violation of s. 501.173, Florida Statutes, may result in an investigation of such violation. The premature release of such information could frustrate or thwart the investigation and impair the ability of the department to effectively and efficiently administer s. 501.173, Florida Statutes. In addition, release of such information before completion of an active investigation could jeopardize the ongoing investigation.

(2) Release of information to which another public record exemption applies once an investigation is completed or ceases to be active would undo the specific statutory exemption protecting that information.

(3) An investigation of a violation of s. 501.173, Florida Statutes, is likely to result in the gathering of sensitive personal information, including identification numbers, unique

identifiers, professional or employment-related information, and personal financial information. Such information could be used for the purpose of identity theft. The release of such information could subject possible victims of data privacy violations to further harm.

(4) Notices received by the department and information received during an investigation of a violation of s. 501.173, Florida Statutes, are likely to contain proprietary information. Such information, including trade secrets, derives independent, economic value, actual, or potential, from being generally unknown to, and not readily ascertainable by, other persons who might obtain economic value from its disclosure or use. Allowing public access to proprietary information, including a trade secret, through a public records request could destroy the value of the proprietary information and cause a financial loss to the controller, processor, or person submitting the information. Release of such information could give business competitors an unfair advantage and weaken the position of the entity supplying the proprietary information in the marketplace.

(5) Information received by the department may contain a computer forensic report or information that could reveal weaknesses in the data security of a controller, processor, or person. The release of this information could result in the identification of vulnerabilities in the cybersecurity system of the controller, processor, or person and be used to harm the

controller, processor, or person and clients.

(6) The harm that may result from the release of information received by the department pursuant to a notification or investigation by the department or a law enforcement agency of a violation of s. 501.173, Florida Statutes, could impair the effective and efficient administration of the investigation and thus, outweighs the public benefit that may be derived from the disclosure of the information.

Section 3. This act shall take effect on the same date that HB 9 or similar legislation takes effect, if such legislation is adopted in the same legislative session or an extension thereof and becomes a law.