HOUSE OF REPRESENTATIVES STAFF ANALYSIS

BILL #: CS/HB 969 Consumer Data Privacy
SPONSOR(S): Regulatory Reform Subcommittee, McFarland
TIED BILLS: HB 971 **IDEN./SIM. BILLS:** SB 1734

REFERENCE	ACTION	ANALYST	STAFF DIRECTOR or BUDGET/POLICY CHIEF
1) Regulatory Reform Subcommittee	18 Y, 0 N, As CS	Wright	Anstead
2) Civil Justice & Property Rights Subcommittee			
3) Commerce Committee			

SUMMARY ANALYSIS

Florida, like most states, has laws requiring businesses to disclose to consumers when a breach of security occurs that affects consumers personal information. In 2014, Florida passed the Florida Information Protection Act (FIPA) that requires commercial and government entities which store or maintain a Floridians' personal information to take reasonable measures to protect such information and report data breaches.

The bill adds "biometric data" to the definition of "personal information" in FIPA. 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.

Due to the growth in the internet and specifically the growth in companies whose entire business model is the collection of personal information for the purpose of selling targeted advertising, many countries and states have adopted or updated their laws relating to the collection and use of personal information. Specifically, the European Union, and states like California, Virginia and Illinois, have enacted data privacy regulations to protect personal information and give consumers more control over how their information is used.

The bill requires certain businesses to publish a privacy policy for personal information.

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 that is readily available to the public from government records or deidentified or aggregate consumer information.

The bill gives consumers certain rights related to personal information collected by a business, 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 requires businesses to comply with certain consumer requests and make certain information available on the business's website.

The bill allows the Department of Legal Affairs to bring an action against, and collect civil penalties from, a business who violates these requirements. Consumers whose personal information is the subject of a data breach may also bring a cause of action against the business in certain limited circumstances.

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

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

FULL ANALYSIS

I. SUBSTANTIVE ANALYSIS

A. EFFECT OF PROPOSED CHANGES:

Florida Information Protection Act – Current Situation

In 2014, Florida passed the Florida Information Protection Act (FIPA).[1] FIPA requires commercial covered entities[2] and government entities which hold personal information to take reasonable measures to protect such information and report data breaches to affected consumers.[3]

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.[4]

Personal information does not include information:

- about an individual that has been made publicly available by a federal, state, or local governmental entity; or
- that is encrypted, secured, or modified to remove elements that personally identify an individual or that otherwise renders the information unusable.[5]

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.[6]

FIPA expressly does not provide a private cause of action, but does authorize enforcement actions under Florida's Unfair and Deceptive Trade Practices Act (FDUTPA) against covered entities for any statutory violations by DLA.[7]

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.

[1] S. 501.171, F.S.; Fla. SB 1524 (2014) (FIPA expanded and updated Florida's data breach disclosure laws contained in s. 817.5681, F.S. (2013), which was adopted in 2005 and repealed in 2014.)
[2] "Covered entity" means a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity that acquires, maintains, stores, or uses personal information. S. 501.171(1)(b), F.S.
[3] Florida Office of the Attorney General, *How to Protect Yourself: Data Security*, http://myfloridalegal.com/pages.nsf/Main/53D4216591361BCD85257F77004BE16C (last visited Mar. 3, 2021).
[4] S. 501.171(1)(g)1., F.S.; OAG *supra* note 22.
[5] S. 501.171(1)(g)2., F.S.
[6] S. 501.171(3)-(6), F.S.
[7] S. 501.171(9), (10), F.S.; OAG *supra* note 22.

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

Florida Deceptive and Unfair Trade Practices Act

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.[8] FDUTPA is based on federal law.[9]

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.[10] 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.[11] In certain circumstances, consumers may also file suit through private actions.[12]

DLA and the SAO have powers to investigate FDUTPA claims, which include:[13]

- 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.[14]

Florida Information Protection Act – Effect of the Bill

The bill adds "biometric data" to the definition of "personal information."

"Biometric data" is defined 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 notify the affected individual, the Department of Legal Affairs (DLA), and credit reporting agencies of a breach of such information. The bill also provides that DLA may bring a FDUTPA action

[8] Chapter 73-124, L.O.F., and s. 501.202, F.S.
[9] 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).
[10] 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 Feb, 21, 2021).
[11] s. 501.203(2), F.S.
[12] s. 501.211, F.S.
[13] S. 501.206(1), F.S.
[14] 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.

against a covered entity which fails to notify DLA of or an individual affected by a breach of biometric information.

Consumer Data Privacy – Current Situation

Consumer Data

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.[15]

From consumer behavior to predictive analytics, companies regularly capture, store, and analyze large amounts of quantitative and qualitative data on their consumer base every day. 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.[16]

Generally, the types of consumer data that businesses collect are:[17]

- Personal data, which includes personally identifiable information, such as Social Security numbers and gender, as well as identifiable information, including your 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.

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).[18] 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.[19]

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 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.[20]

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.

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. [21]

---

[15] 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.
[16] *Id*.
[17] *Id*.
[18] 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 Mar. 3, 2021).
[19] *Id*.
[20] 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 Mar. 6, 2021).
[21] TechRepublic, GDPR: A cheat sheet, https://www.techrepublic.com/article/the-eu-general-data-protection-regulation-gdpr-the-smart-persons-guide/ (last visited Mar. 6, 2021).

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.[22]

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.[23]

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.[24]

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:[25]

- 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:[26]

- 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% or more of their annual revenue from selling California residents' personal information.

Businesses are required to give consumers certain notices explaining their privacy practices and provide certain mechanisms to allow consumers to exercise their rights.[27]

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.[28] As of July 2020, approximately 50 suits had been filed pursuant to this provision.[29]

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:[30]

---

[22] *Id*.
[23] *Id*.
[24] *Id*.
[25] State of California Department of Justice, Office of the Attorney General, California Consumer Privacy Act (CCPA), https://oag.ca.gov/privacy/ccpa (last visited Mar. 6, 2021).
[26] Cal. Civ. Code § 1798.140.
[27] Cal. Civ. Code §§ 1798.130, 1798.135.
[28] Cal. Civ. Code §§ 1798.150, 1798.155.
[29] Holland & Knight LLP, Litigating the CCPA in Court, https://www.hklaw.com/en/insights/publications/2020/07/litigating-the-ccpa-in-court (last visited Mar. 6, 2021).
[30] 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 Mar. 6, 2021).

- Allows 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% 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.[31] The VCDPA, which will not become effective until January 1, 2023, borrows heavily from CCPA and GDPR.[32] 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 is less prescriptive and more straightforward than its predecessors, and potentially may be a lighter implementation task for companies.[33]

Generally, with regard to personal data, the VCDPA grants consumers the right to:
- access,
- correct,
- delete,
- obtain a copy of, and
- to opt out of the processing of personal data for the purposes of targeted advertising.

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.[34]

Comparison of The GDPR, CCPA as amended by the CPRA, and VCDPA

[31] 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 Mar. 6, 2021).
[32] 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 Mar. 6, 2021).
[33] *Id*.
[34] Virginia's Legislative Information System, Bill Summary for SB 1392, https://lis.virginia.gov/cgi-bin/legp604.exe?211+sum+SB1392S (last visited Mar. 6, 2021).

	VCDPA	CCPA, as amended by the CPRA	GDPR
Right to opt-out of sale	✓	✓	✗
Opt-in or opt-out for processing of sensitive information	Opt-in	Opt-out	Opt-in
Statutory cure period for violations	✓	✓	✗
Right to appeal denials of requests	✓	✗	✗
Express obligations regarding de-identified data	✓	✗	✗
Requirement to perform data protection impact assessments	✓	✓	✓
Private right of action	✗	✓	✓
Governmental enforcement entities	Attorney General	CPPA, Attorney General	DPAs
Penalties	Up to $7,500 per violation	Up to $2,500 per violation and up to $7,500 per intentional violation or violation involving minors	Up to €10 million, or 2% of worldwide annual revenue from the preceding financial year, whichever amount is higher, in the case of less severe violations. Up to €20 million, or 4% of worldwide annual revenue from the preceding financial year, whichever amount is higher, in the case of more serious violations.
Operative date	January 1, 2023	January 1, 2023	May 25, 2018

[35]

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 US to specifically regulate biometrics.

Under BIPA, a private entity:[36]

- 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.
- 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.

BIPA provides a private cause of action, with relief including:[37]

- 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;

[35] JDSupra, *Virginia Is For Lovers…Of Data Privacy*, https://www.jdsupra.com/legalnews/virginia-is-for-lovers-of-data-privacy-3879845/ (last visited Mar. 6, 2021).
[36] 740 Ill. Comp. Stat. 14/10, 14/15 (2008).
[37] 740 Ill. Comp. Stat. 14/20 (2008).

- 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.[38] 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.[39]

Federal Laws Addressing Data Privacy

While there is no broad federal law addressing data privacy, there are several laws that address the need to keep certain data private or protected in various industries.

Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act of 1996 (HIPAA)[40] 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 US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule[41] to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.[42]

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.[43]

"Individually identifiable health information" is information, including demographic data, that relates to:[44]
- 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.[45] 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 is called "electronic protected health 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:[46]
- 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.

---

[38] *Rosenbach v. Six Flags Entertainment Corporation*, 2019 IL 123186.
[39] *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).
[40] 42 U.S.C. § 1320.
[41] 45 C.F.R. §§ 160 and 164.
[42] 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 Mar. 6, 2021).
[43] *Id*.
[44] 45 C.F.R. § 160.103.
[45] 20 U.S.C. § 1232(g).
[46] CDC, supra note 43.

"Covered entities" who must abide by the Privacy Rule and the Security Rule are:[47]

- 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 United States Food and Drug Administration (FDA).[48] The 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 Rule has not been substantively updated since 1991.[49] Among other requirements, the Common Rule mandates that researchers protect the privacy of subjects and maintain confidentiality of human subject data.[50]

The FDA is a member of the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use (Council), which brings together the regulatory authorities and pharmaceutical industry to develop guidelines for pharmaceutical trials.[51]

The Fair Credit Reporting Act

The Fair Credit Reporting Act[52] (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.[53]

The Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act[54] 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.[55]

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 has opt-out rights from having their nonpublic personal information shared with third parties.[56]

---

[47] 45 C.F.R. §§ 160.102, 160.103.
[48] 21 C.F.R. §§ 50, 60.
[49] 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 Mar. 6, 2021).
[50] 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 Mar. 6, 2021).
[51] International Council for Harmonisation, Welcome to the ICH Official Website, https://www.ich.org/ (last visited Mar. 6, 2021).
[52] 15 U.S.C. § 1681.
[53] The Federal Trade Commission, Fair Credit Reporting Act, https://www.ftc.gov/enforcement/statutes/fair-credit-reporting-act (last visited Mar. 6, 2021).
[54] 15 U.S.C. § 6801.
[55] 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 Mar. 6, 2021).

Driver's Privacy Protection Act

The Driver's Privacy Protection Act of 1994 (DPPA)[57] protects the privacy of personal information assembled by State Department 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 department 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.[58]

DPPA also requires states to get permission from individuals before their personal motor vehicle record may be sold or released to third-party marketers.[59]

Family Educational Rights and Privacy Act

The Family Educational Rights and Privacy Act (FERPA)[60] 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 reaches the age of 18 or attends 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.[61]

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 by a business,
- 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 business that receives a verifiable consumer request to access, delete, correct, or opt-out must comply with such consumer request, with certain exceptions.

---

[56] 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 visted Mar. 6, 2021).
[57] 18 U.S.C. § 2721.
[58] 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 Mar. 6, 2021).
[59] *Id*.
[60] 20 U.S.C. § 1232(g); 34 C.F.R. § 99.
[61] 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 Mar. 6, 2021).

Businesses may share personal information with a service provider, even if a consumer has "opted-out," if the service provider processes information on behalf of a business for a defined business purpose pursuant to a written contract which limits how the service provider uses such information.

DLA may bring an action against a business who violates the provisions of the bill, and such business may be subject to certain civil penalties. A consumer may bring a private cause of action only in the instance of a breach of personal data.

Definitions

The bill includes the following definitions:

- "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 or household, including via a device. The term does not include one or more individual consumer records that have been deidentified.
- "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.
- "Business" 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 one 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 for the business's commercial purposes, sells, or shares for commercial purposes, the personal information of 50,000 or more consumers, households, or devices.
            - 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 a business and that shares common branding with the business. As used in this subparagraph, 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 business;
            - 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.
        - "Common branding" means a shared name, servicemark, or trademark.
- "Business purpose" means the use of personal information for the operational purpose of a business or service provider, or other notified purposes, provided that the use of personal information is reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed or for another operational purpose

that is compatible with the context in which the personal information was collected. The term includes:
    - Auditing relating to a current interaction with a consumer and concurrent transactions, including, but not limited to, counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards.
    - Detecting security incidents; protecting against malicious, deceptive, fraudulent, or illegal activity; and prosecuting those responsible for that activity.
    - Debugging to identify and repair errors that impair existing intended functionality.
    - Short-term, transient use, provided that the personal information is not disclosed to another third party and is not used to build a profile about a consumer or otherwise alter an individual consumer's experience outside the current interaction, including, but not limited to, the contextual customization of ads shown as part of the same interaction.
    - Performing services on behalf of the business or service provider, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, or providing similar services on behalf of the business or service provider.
    - Undertaking internal research for technological development and demonstration.
    - Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business.
- "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.
- "Commercial purposes" means to advance the commercial or economic interests of a person, such as inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or directly or indirectly enabling or effecting a commercial transaction.
- "Consumer" means a natural person who resides in or is domiciled in this state, however identified, including by any unique identifier, and who is:
    - In this state for other than a temporary or transitory purpose; or
    - Domiciled in this state but resides outside this state for a temporary or transitory purpose.
- "Deidentified" means information that does not reasonably identify, relate to, or describe a particular consumer, or is not reasonably capable of being directly or indirectly associated or linked with a particular consumer, provided that a business that uses deidentified information:
    - Implements technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.
    - Implements business processes that specifically prohibit reidentification of the information.
    - Implements business processes to prevent inadvertent release of deidentified information.
    - Does not attempt to reidentify the information.
- "Personal information" means 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 includes, but is not limited to, the following:
        - Identifiers such as a real name, alias, postal address, unique identifier, online identifier, internet protocol address, email address, account name, social security number, driver license number, passport number, or other similar identifiers.
        - Information that identifies, relates to, or describes, or could be associated with, a particular individual, including, but not limited to, a name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver license or state identification card number, insurance policy number, education, employment, employment history, bank

account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information.
        - Characteristics of protected classifications under state or federal law.
        - Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
        - Biometric information.
        - Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet website, application, or advertisement.
        - Geolocation data.
        - Audio, electronic, visual, thermal, olfactory, or similar information.
        - Professional or employment-related information.
        - Education information that is not publicly available, personally identifiable information as defined in the Family Educational Rights and Privacy Act, 20 U.S.C. s. 1232(g) and 34 C.F.R. part 99.
        - Inferences drawn from any of the information identified in this paragraph to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.
    - The term does not include consumer information that is:
        - Publicly and lawfully made available from federal, state, or local government records.
        - Deidentified or aggregate consumer information.
- "Probabilistic identifier" means the identification of a consumer or a device to a degree of certainty of more probable than not based on any categories of personal information.
- "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 business to another business or a third party for monetary or other valuable consideration.
- "Service provider" 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 business and to which the business discloses a consumer's personal information for a business purpose 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 business, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business.
- "Share" 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 business and a third party for advertising for the benefit of a business.
- "Third party" means a person who is not any of the following:
    - The business that collects personal information from consumers.
    - A service provider to whom the business discloses personal information about consumers for a business purpose pursuant to a written contract.
- "Unique identifier" means a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers which can be used to identify a particular consumer or device linked to a consumer or

family. As used in this paragraph, the term "family" means a custodial parent or guardian and any minor children of whom the parent or guardian has custody, or a household.

- "Verifiable consumer request" means a request that is made by a consumer, by a consumer on behalf of the consumer's minor child, or by a natural person or a person authorized by the consumer to act on the consumer's behalf, and that the business can reasonably verify pursuant to rules adopted by the department to be the consumer about whom the business has collected personal information. A business is not obligated to provide information to the consumer if the business cannot verify that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by the consumer to act on the consumer's behalf.

Business Privacy Policies

The bill requires a business that collects personal information about consumers to maintain an online privacy policy, make such policy available on its Internet website, and update the information at least once every 12 months. The online privacy policy must include the following information:

- Any Florida-specific consumer privacy rights.
- A list of the categories of personal information the business collects or has collected about consumers.
- Of the identified categories, a list that identifies which categories of personal information the business sells or shares or has sold or shared about consumers. If the business does not sell or share personal information, the business must disclose that fact.
- Of the identified categories, a list that identifies which categories of personal information the business discloses or shares or has disclosed or shared about consumers for a business purpose. If the business does not disclose or share personal information for a business purpose, the business must disclose that fact.
- The right to opt-out of the sale or sharing to third parties and the ability to request deletion or correction of certain personal information.

A consumer has the right to request that a business that collects personal information disclose to the consumer the categories and specific pieces of personal information the business collects from or about consumers.

A business that collects personal information must, 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. A business may not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice.

A business must provide and follow a retention schedule that prohibits the use and retention of personal information after satisfaction of the initial purpose for collecting or obtaining such information, or after the duration of a contract, or 1 year after the consumer's last interaction with the business, whichever occurs first. This paragraph does not apply to biometric information used for ticketing purposes and does not apply if such information is only kept for the time related to the duration of the ticketed event.

Consumer Right to Request Personal Information Collected

The bills provides that a consumer has the right to request that a business that collects personal information about the consumer disclose the personal information that has been collected by the business.

The bill requires a business that receives a verifiable consumer request from a consumer to access personal information to promptly take steps to disclose and deliver, free of charge to the consumer, the personal information requested. The information may be delivered by mail or electronically, and if provided electronically, the information must be in a portable and, to the extent technically feasible, readily useable format that allows the consumer to transmit this information to another entity without

hindrance. A business 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.

Specifically, the bill requires a business to disclose the following to the consumer:

- The specific pieces of personal information it has collected about the consumer.
- The categories and sources from which it collected the consumer's personal information.
- The business or commercial purpose for collecting or selling the consumer's personal information.
- The categories of third parties which the business shares the consumer's personal information.

The bill does not require a business to do the following:

- Retain any personal information about a consumer collected for a single one-time transaction if, in the ordinary course of business, that information about the consumer is not retained.
- 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.

Consumer Right to Correct or Delete Personal Information

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

The bill requires a business that receives a verifiable consumer request from a consumer to delete the consumer's personal information to delete the consumer's personal information from its records and direct any service providers to delete the consumer's personal information from their records, unless it is reasonably necessary for the business or service provider 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 within the context of a business' ongoing business relationship with the consumer, or otherwise perform a contract between the business 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 business' 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 business.
- Comply with a legal obligation.
- As reasonably needed to protect the business’s interests against existing legal disputes, legal action, or governmental investigations.
- Otherwise internally use the consumer's personal information in a lawful manner that is compatible with the context in which the consumer provided the information.

The bill provides that a consumer has the right to request a business that maintains inaccurate personal information about the consumer to correct the inaccurate personal information, taking into account the nature of the personal information and the purposes of the processing of the personal information. A business 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. If a business maintains a self-service mechanism to allow a consumer to correct certain personal information, the business may require the consumer to correct their own personal information through such mechanism.

Consumer Right to Request Personal Information Sold or Shared

The bill provides that a consumer has the right to request that a business that sells or shares personal information about the consumer, or discloses such information for a business purpose, to disclose to the consumer upon receipt of a verifiable consumer request:

- The categories of personal information about the consumer the business sold or shared.
- The categories of third parties to which the personal information about the consumer was sold or shared by category of personal information for each category of third parties to which the personal information was sold or shared.
- The categories of personal information about the consumer that the business disclosed for a business purpose.

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 business unless the consumer has received explicit notice and is provided an opportunity to opt-out.

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

The bill provides that a consumer has the right at any time to direct a business 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 business 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 business may not sell or share the personal information of a consumer if the business has actual knowledge that the consumer is not 16 years of age or older, unless the consumer, in the case of consumers between 13 and 15 years of age, or the consumer's parent or guardian, in the case of consumers who are 12 years of age or younger, has affirmatively authorized the sale or sharing of the consumer's personal information. A business that willfully disregards the consumer's age is deemed to have had actual knowledge of the consumer's age.

The bill provides that a business that has received direction from a consumer prohibiting the sale or sharing of the consumer's personal information or that has not received consent to sell or share a minor consumer's personal information is prohibited from selling or sharing the consumer's personal information after its receipt of the consumer's direction, unless the consumer subsequently provides express authorization for the sale or sharing of the consumer's personal information.

The bill provides that a business does not sell personal information when:

- A consumer uses or directs the business to intentionally disclose personal information or uses the business to intentionally interact with a third party. An intentional interaction occurs when the consumer intends to interact with the third party, via 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.
- The business uses or shares an identifier for a consumer who has opted out of the sale or sharing of the consumer's personal information for the purposes of alerting third parties that the consumer has opted out of the sale or sharing of the consumer's personal information.
- The business uses or shares with a service provider personal information of a consumer that is necessary to perform a business purpose if both of the following conditions are met:
    - The business has provided notice that the personal information of the consumer is being used or shared in its terms and conditions.
    - The service provider does not further collect, sell, share, or use the personal information of the consumer except as necessary to perform the business purpose.
- The business transfers to a third party the personal information of a consumer 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 business. 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 promises made at the time of collection, it must provide prior notice of the new or changed practice to the consumer. The notice must be sufficiently prominent and robust to ensure that existing consumers can easily exercise their choices consistently with the bill.

The bill provides that a business does not share personal information when:

- A consumer uses or directs the business to intentionally disclose personal information or intentionally interact with one or more third parties.
- The business uses or shares an identifier for a consumer who has opted-out of sharing the consumer's personal information for the purposes of alerting persons that the consumer has opted-out of sharing the consumer's personal information.

Discrimination Against Consumers Who Exercise Their Rights

The bill provides that a business may not discriminate against a consumer who exercised any of the consumer's rights provided for in the bill. Discrimination includes, but is not limited to:

- Denying goods or services to the consumer.
- Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.
- Providing a different level or quality of goods or services to the consumer.
- Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.

The bill does not prohibit a business from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the business by the consumer's data.

The bill provides that a business may:

- offer financial incentives, including payments to consumers as compensation, for the collection, sale, or deletion of personal information.
- offer a different price, rate, level, or quality of goods or services to the consumer if the price or difference is directly related to the value provided to the business by the consumer's personal information.

A business that offers any financial incentives must notify consumers of the financial incentives and may enter a consumer into a financial incentive program only if the consumer gives the business 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 provides that a business may not use financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature.

Requests for Personal Information

The bill requires businesses to, in a form that is reasonably accessible to consumers, make available two or more methods for submitting verifiable consumer requests, including, but not limited to, a toll-free number and, if the business maintains an Internet website, a link on the homepage of the website. The business may not require the consumer to create an account with the business in order to make a verifiable consumer request.

The bill requires the business to deliver the information required or to act on the request to a consumer free of charge within 45 days after receiving a verifiable consumer request. The response period may be extended once by 30 additional days when reasonably necessary, taking into account the complexity of the consumer's requests, provided the business informs the consumer of any such extension within the initial 45-day response period along with the reason for the extension. The information must be delivered in a readily usable format that allows the consumer to transmit the information from one entity to another entity without hindrance.

The bill provides that if a third party assumes control of all or part of a business and acquires a consumer's personal information as part of the transfer, and the third party materially alters how it uses a consumer's personal information or shares the information in a manner that is materially inconsistent with the promises made at the time of collection, the third party must provide prior notice of the new or changed practice to the customer. The notice must be sufficiently prominent and robust to ensure that existing consumers can easily exercise their choices.

The bill requires that any contract between a business and a service provider must prohibit the service provider from:

- Selling or sharing the personal information;
- Retaining, using, or disclosing the personal information for any purpose other than for the business purposes specified in the contract for the business, including retaining, using, or disclosing the personal information for a commercial purpose other than the business purposes specified in the contract with the business; or
- Combining the personal information that the service provider receives from or on behalf of the business with personal information that it receives from or on behalf of another person or entity or that the service provider collects from its own interaction with the consumer, provided that the service provider may combine personal information to perform any business purpose.

The bill requires that a third party that receives personal information is prohibited from:

- Selling or sharing the personal information; or
- Retaining, using, or disclosing the information outside of the direct business relationship between the person and the business.

A third party or a service provider must require any subcontractor to meet the same obligations of such third party or service provider with respect to personal information.

The bill provides that a third party or service provider or any subcontractor thereof who violates any of the restrictions is liable for any violations. A business that discloses personal information to a third party or service provider in compliance with certain provisions is not liable if the person receiving the personal information uses it in violation of the restrictions, provided that at the time of disclosing the personal information, the business does not have actual knowledge or reason to believe that the person intends to commit such a violation.

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

The bill requires a business to, in a form that is reasonably accessible to consumers:

- Provide a clear and conspicuous link on the business'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 business may not require a consumer to create an account in order to direct the business not to sell the consumer's personal information.
- Include a description of a consumer's rights along with a separate link to the "Do Not Sell or Share My Personal Information" Internet webpage in:
    - Its online privacy policy or policies
    - Any Florida-specific consumer privacy rights.
- Ensure that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with certain provisions are informed of all requirements and how to direct consumers to exercise certain rights.
- For consumers who opt-out of the sale or sharing of their personal information, refrain from selling or sharing personal information collected by the business about the consumer.
- 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 of the consumer's personal information.

- 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 does not require a business to include the required links and text on the homepage that the business makes available to the public generally, if the business maintains a separate and additional homepage that is dedicated to Florida consumers, and the business takes reasonable steps to ensure that Florida consumers are directed to the homepage for Florida consumers.

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 business 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.

Exceptions

The bill does not restrict any business' or third party's ability to do any of the following:

- Comply with federal, state, or local laws.
- Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities.
- Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law.
- Exercise legal rights or privileges.
- Collect, use, retain, sell, or disclose deidentified personal information or aggregate consumer information. If a business uses deidentified information, the business must:
    - A Implement technical safeguards that prohibit reidentification of the consumer to whom the information may pertain;
    - Implement business processes that specifically prohibit reidentification of the information;
    - Implement business processes to prevent inadvertent release of deidentified information; and
    - Not attempt to reidentify the information.

This bill does not apply to:

- A business that collects or discloses its employees', applicants', interns' or volunteers' personal information, so long as the business is collecting or disclosing such information within the scope of its role as an employer.
- Health information that is collected by 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.
- A covered entity or business associate governed by the privacy, security, and breach notification rules issues by the United States Department of Health and Human Services in 45 C.F.R. parts 160 and 164, to the extent the covered entity or business associate maintains patient information in the same manner as medical information or protected health information as described in subparagraph 2.
- Information collected as part of a clinical trial subject to the Federal Policy for the Protection of Human Subjects pursuant to good clinical practice guidelines issued by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use or pursuant to human subject protection requirements of the United States Food and Drug Administration.
- Sale or sharing of personal information to or from a consumer reporting agency if that information is to be reported in or used to generate a consumer report as defined by 15 U.S.C. s. 1681(a), and if use of that information is limited by the federal Fair Credit Reporting Act, 15 U.S.C. s. 1681 et seq.
- 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.

- 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.

"Research" means scientific, systematic study and observation, including, but not limited to, basic research or applied research that is in the public interest and that adheres to all other applicable ethics and privacy laws or studies conducted in the public interest in the area of public health. Research with personal information that may have been collected from a consumer in the course of the consumer's interactions with a business's service or device for other purposes must be:

- Compatible with the business purpose for which the personal information was collected.
- Subsequently pseudonymized and deidentified, or deidentified and in the aggregate, such that the information does not reasonably identify, relate to, or describe, or is not capable of being directly or indirectly associated or linked with, a particular consumer.
- Made subject to technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.
- Subject to business processes that specifically prohibit reidentification of the information.
- Made subject to business processes to prevent inadvertent release of deidentified information.
- Protected from any reidentification attempts.
- Used solely for research purposes that are compatible with the context in which the personal information was collected and not used for any commercial purpose.
- Subjected by the business conducting the research to additional security controls that limit access to the research data to only those individuals in a business necessary to carry out the research purpose.

"Pseudonymize" means the processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable consumer.

Applicability to Contracts

The bill provides that any provision of a contract or agreement of any kind 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. This provision of the bill does not prevent a consumer from declining to request information from a business, declining to opt-out of a business's sale or sharing of the consumer's personal information, or authorizing a business to sell or share the consumer's personal information after previously opting out. These provisions only apply to contracts entered into after January 1, 2022.

Private Cause of Action

The bill allows a consumer whose nonencrypted and nonredacted personal information or e-mail address, in combination with a password or security question and answer that would allow access to the account, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of a business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information to bring a civil action for any of the following:

- 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, as the court deems proper.

Enforcement and Implementation

The bill provides that upon belief that any business, service provider, or other person or entity is in violation and that proceedings would be in the public interest, DLA may bring an action against such business, service provider, or other person or entity and may seek a civil penalty of not more than $2,500 for each unintentional violation or $7,500 for each intentional violation. Such fines may be tripled if the violation involves a consumer who is 16 years of age or younger. A business may be found to be in violation of the bill if it fails to cure any alleged violation within 30 days after being notified in writing by DLA of the alleged noncompliance.

DLA may adopt rules to implement certain provisions of the bill.

The bill provides an effective date of January 1, 2022.

B. SECTION DIRECTORY:

Section 1: Amends s. 501.171, F.S.; relating to FIPA and what kind of breached information triggers notification requirements.
Section 2: Creates s. 501.173, F.S., relating to consumer data privacy rights and requirements for businesses who collect personal information.
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 from civil penalties collected by DLA.

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

On March 10, 2021, the Regulatory Reform Subcommittee adopted five amendments and reported the bill favorably as a committee substitute. The committee substitute:

- Clarifies the definition of “third party,”
- Clarifies the definition for “unique identifier” by including “linked to a consumer or family” used elsewhere in the bill,
- Allows consumers to self-correct information if the business provides a mechanism,
- Clarifies that business records may be retained for an existing legal dispute,
- Provides that businesses and service providers are not required to delete personal information under certain circumstances,
- Clarifies that certain intentional actions do not qualify as selling personal information,
- Removes requirements that certain provisions be included in a third party contract,
- Removes duplicate provisions,
- Clarifies the time period for complying with a consumer request,
- Adds the words “business associate” to conform to another provision in the bill, and
- Adds applicants, interns, and volunteers to the list of types of employees under the employer exception.

This analysis is drafted to the committee substitute as passed by the Regulatory Reform Subcommittee