HOUSE OF REPRESENTATIVES STAFF ANALYSIS

BILL #: CS/CS/CS/HB 969 Consumer Data Privacy
SPONSOR(S): Commerce Committee, Civil Justice & Property Rights Subcommittee, Regulatory Reform Subcommittee, McFarland, and others
TIED BILLS: CS/CS/HB 971 **IDEN./SIM. BILLS:**

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	17 Y, 0 N, As CS	Mathews	Jones
3) Commerce Committee	22 Y, 0 N, As CS	Wright	Hamon

SUMMARY ANALYSIS

Florida, like most states, has laws requiring businesses to disclose to consumers when a breach of security occurs that affects a consumer's personal information. In 2014, Florida passed the Florida Information Protection Act (FIPA) that requires commercial and government entities which store or maintain a Floridian's 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 controllers 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, certain employee information, or deidentified or aggregate information.

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

The bill allows the Department of Legal Affairs to bring an action against, and collect civil penalties from, a controller, processor, or person who violates these requirements. Consumers whose personal information has been breached, sold, or shared after opting-out, or retained after a request to delete or correct may also bring a cause of action against the controller, processor, or person 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 July 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 by DLA under Florida's Unfair and Deceptive Trade Practices Act (FDUTPA) against covered entities for any statutory violations.[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. 24, 2021).
[4] *Id*.; S. 501.171(1)(g)1., F.S.
[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 3.

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]

FDUTPA may not be applied to certain entities in certain circumstances, including:[15]

- 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.

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,

[8] Ch. 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 Mar. 24, 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.
[15] S. 501.212(4), F.S.

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 such information. The bill also provides that DLA may bring a FDUTPA action 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 of day-to-day operations, making more informed business decisions and learning about their customers.[16]

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.[17]

Generally, the types of consumer data that businesses collect are:[18]

- 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.

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).[19] 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.[20]

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.[21]

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.

---

[16] 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 Mar. 24, 2021).
[17] *Id*.
[18] *Id*.
[19] 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. 24, 2021).
[20] *Id*.
[21] 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. 24, 2021).

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. [22]

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.[23]

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.[24]

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.[25]

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:[26]

- 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:[27]

- 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.

Businesses are required to give consumers certain notices explaining their privacy practices and provide certain mechanisms to allow consumers to exercise their rights.[28]

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.[29] As of July 2020, approximately 50 suits had been filed pursuant to this provision.[30]

---

[22] TechRepublic, GDPR: A cheat sheet, https://www.techrepublic.com/article/the-eu-general-data-protection-regulation-gdpr-the-smart-persons-guide/ (last visited Mar. 24, 2021).
[23] *Id*.
[24] *Id*.
[25] *Id*.
[26] 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. 24, 2021).
[27] Cal. Civ. Code § 1798.140.
[28] Cal. Civ. Code §§ 1798.130, 1798.135.
[29] Cal. Civ. Code §§ 1798.150, 1798.155.
[30] 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. 24, 2021).

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:[31]

- 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.[32] The VCDPA, which will not become effective until January 1, 2023, borrows heavily from CCPA and GDPR.[33] 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.[34]

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.[35]

---

[31] 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. 24, 2021).
[32] 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. 24, 2021).
[33] 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. 24, 2021).
[34] *Id*.
[35] Virginia's Legislative Information System, Bill Summary for SB 1392, https://lis.virginia.gov/cgi-bin/legp604.exe?211+sum+SB1392S (last visited Mar. 24, 2021).

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

	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

[36]

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:[37]

- 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.

BIPA provides a private cause of action, with relief including:[38]

- liquidated damages of $1,000 or actual damages, whichever is greater, against a private entity that negligently violates BIPA;

[36] JDSupra, *Virginia Is For Lovers…Of Data Privacy*, https://www.jdsupra.com/legalnews/virginia-is-for-lovers-of-data-privacy-3879845/ (last visited Mar. 24, 2021).
[37] 740 Ill. Comp. Stat. 14/10, 14/15 (2008).
[38] 740 Ill. Comp. Stat. 14/20 (2008).

- 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.[39] 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.[40]

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)[41] 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[42] to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.[43]

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.[44]

"Individually identifiable health information" is information, including demographic data, that relates to:[45]
- 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.[46] 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 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:[47]
- Ensure the confidentiality, integrity, and availability of all electronic protected health information,
- Detect and safeguard against anticipated threats to the security of the information,

[39] *Rosenbach v. Six Flags Entertainment Corporation*, 2019 IL 123186.
[40] *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).
[41] 42 U.S.C. § 1320.
[42] 45 C.F.R. §§ 160 and 164.
[43] 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. 24, 2021).
[44] *Id*.
[45] 45 C.F.R. § 160.103.
[46] 20 U.S.C. § 1232(g).
[47] CDC, supra note 42.

- 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:[48]
- 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).[49] 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.[50] Among other requirements, the Common Rule mandates that researchers protect the privacy of subjects and maintain confidentiality of human subject data.[51]

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.[52]

The Fair Credit Reporting Act

The Fair Credit Reporting Act[53] (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.[54]

The Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act[55] 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.[56]

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.[57]

---

[48] 45 C.F.R. §§ 160.102, 160.103.
[49] 21 C.F.R. §§ 50, 60.
[50] 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. 24, 2021).
[51] 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. 24, 2021).
[52] International Council for Harmonisation, Welcome to the ICH Official Website, https://www.ich.org/ (last visited Mar. 24, 2021).
[53] 15 U.S.C. § 1681.
[54] The Federal Trade Commission, Fair Credit Reporting Act, https://www.ftc.gov/enforcement/statutes/fair-credit-reporting-act (last visited Mar. 24, 2021).
[55] 15 U.S.C. § 6801.
[56] 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. 24, 2021).

Driver's Privacy Protection Act

The Driver's Privacy Protection Act of 1994 (DPPA)[58] 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.[59]

DPPA also requires states to get permission from individuals before their personal motor vehicle record may be sold or released to third-party marketers.[60]

Family Educational Rights and Privacy Act

The Family Educational Rights and Privacy Act (FERPA)[61] 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.[62]

Children's Online Privacy Protection Act (COPPA)

The Children's Online Privacy Protection Act (COPPA)[63] 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.[64]

COPPA requires covered entities to:[65]

- Give parents direct notice of their privacy policies, including a description of their data collection and sharing practices;

---

[57] 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 visited Mar. 24, 2021).
[58] 18 U.S.C. § 2721.
[59] 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. 24, 2021).
[60] *Id*.
[61] 20 U.S.C. § 1232(g); 34 C.F.R. § 99.
[62] 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. 24, 2021).
[63] 16 C.F.R. pt. 312.
[64] 15 U.S.C. §§ 6502(a)-(b).
[65] *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 Apr. 7, 2021).

- 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.[66]

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.

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.

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:

[66] 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 Apr. 7, 2021).

- 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, 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.

  - 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 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 consumer information that is:
  - Publicly and lawfully made available.
  - Deidentified or aggregate consumer information.
  - Employment information.
- "Probabilistic identifier".
- "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.
- "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.
- "Research".
- "Pseudonymize".
- "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".
- "Unique identifier".
- "Verifiable consumer request".

Exceptions

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

- Collect and transmit personal information 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.
- 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 controller, processor, 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 controller uses deidentified information, the controller must:
    - 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:

- 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.

Privacy Policies

The bill requires a controller that collects personal information about consumers to maintain an online privacy policy, make such policy available from its homepage, and update the information at least once every 12 months unless the privacy policy has not changed and an update is not reasonably required. 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.
- Of the categories identified, a list that identifies which categories of personal information the controller sells or shares or has sold or shared about consumers. If the controller does not sell or share personal information, the controller must disclose that fact.
- 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 provides that a consumer has the right to request that a controller disclose to the consumer the categories of personal information the controller collects from or about consumers, and such request does not need to be a verified consumer request.

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. A controller that does not collect personal information directly from the consumer does not need to provide a notice at collection to the consumer if it does not sell or share the consumer’s personal information.

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 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 2 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.

Consumer Right to Request 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 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 categories of sources from which it collected the consumer's personal information.
- The purpose for collecting, selling, or sharing the consumer's personal information.
- The categories of third parties which the controller shares the consumer's personal information.

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

- The categories of personal information about the consumer the controller sold or shared.
- The categories of third parties to which the personal information about the consumer was sold or shared.
- The categories of personal information about the consumer that the controller 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 provides that a controller is not required 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.

The bill requires a controller 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 controller maintains an Internet website, a link on the homepage of the website. The controller may not require the consumer to create an account with the controller in order to make a verifiable consumer request.

The bill requires the controller to deliver the information required or act on the request for information 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, while taking into account the complexity of the consumer's requests, provided the controller 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 person to another person without hindrance.

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 from a consumer to delete the consumer's personal information to delete the consumer's personal information from its records and direct any processors to delete the such information, unless 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 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.
- Comply with a legal obligation.
- As reasonably needed to protect the controller'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 controller 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 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. 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 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 the 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. This right may be referred to as the right to opt-in. A controller that complies with the verifiable parental consent requirements of COPPA is be deemed compliant with any obligation to obtain parental consent.

The bill provides that a controller 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 controller does not sell or share personal information when:

- The controller discloses personal information to another controller, a processor, or a government entity 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.
- A consumer uses or directs the controller to intentionally disclose personal information 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, 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 controller 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 controller uses or shares with a processor personal information of a consumer that is necessary to perform a contracted purpose if both of the following conditions are met:
    - The controller has provided notice that the personal information of the consumer is being used or shared in its terms and conditions.
    - The processor does not further collect, sell, share, or use the personal information of the consumer except as necessary to perform the contracted purpose.
- The controller 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 controller. 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.

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

The bill requires a controller to:

- 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.
- In a form that is reasonably accessible to consumers, 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, and
    - Any Florida-specific consumer privacy rights.

- Ensure that all individuals responsible for handling consumer inquiries about the controller's privacy practices or the controller'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 controller 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 controller to include the required links and text on the homepage that the controller makes available to the public generally, if the controller maintains a separate and additional homepage that is dedicated to Florida consumers, and the controller 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 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.

Discrimination Against Consumers Who Exercise Their Rights

The bill provides that a controller 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 controller 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 controller by the consumer's data or is related to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.

The bill provides that a controller may:

- Offer financial incentives, including payments to consumers as compensation, for the collection, sale, or deletion of personal information; and
- 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 controller by the consumer's personal information or is related to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.

A controller 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 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 provides that a controller may not use 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 or sharing the personal information;
- Prohibit the processor from retaining, using, or disclosing the personal information other than for the purposes specified in the contract with the controller;
- Prohibit the processor from combining the personal information that the processor receives from or on behalf of the controller with personal information that it receives from or on behalf of another person or that the processor collects from its own interaction with the consumer, provided that the processor may combine personal information to perform any purpose specified in the contract and such combination is reported to 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 to demonstrate compliance.

The bill provides that 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. Irrespective of the terms of the arrangement or contract, the consumer may exercise his or her rights against a controller or a processor that does not act in accordance with the terms of the contract with the controller. 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.

The bill provides that a third party or processor or any subcontractor thereof who violates any of the restrictions imposed upon it is liable or responsible for any failure to comply with the requirements of the bill. A controller that discloses personal information to a third party or processor in compliance with the bill is not liable or responsible if the person receiving the personal information uses it without complying with the requirements of the bill, if the controller does not have actual knowledge or reason to believe that the person intends to not comply.

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 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.

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 protect a consumer's 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 consumer's account, and is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of a controller's violation of the duty to implement and maintain reasonable security procedures and practices;

- 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; or
- Continuing to sell or share a consumer's personal information after the consumer chooses to opt-out.

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 which inures to the benefit of a consumer does not arise from the failure of a controller, processor or person to comply with the requirements of the bill and evidence of such may only be used to prove such a private or DLA cause of action.

Enforcement and Implementation

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.

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 to the controller, processor, or person that indicates that the controller, processor, or person will not be offered a 45-day cure period for any future violations. 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.

DLA may adopt rules to implement the bill.

The bill provides an effective date of July 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 controllers 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.

On March 23, 2021, the Civil Justice & Property Rights Subcommittee adopted seven amendments and reported the bill favorably as a committee substitute. The committee substitute:

- Removes duplicative language related to business purposes;
- Broadens the definition of “publicly and lawfully available;”
- Clarifies that a business does not need to annually update their privacy policy if there have not been any changes;
- Requires a business that collects a consumer’s personal information to implement and maintain reasonable security procedures and practices;
- Clarifies the exceptions for medical information;
- Clarifies the exception for information related to consumer report;
- Adds an exception for transactional uses of information for payment purposes;
- Adds an exception for first party advertising;
- Allows a consumer to bring a civil action against and receive relief from a business for:
    - Continuing to sell or share personal information after opting-out; and
    - Failing to delete or correct information under certain circumstances; and
- Allows the Attorney General to grant a discretionary 30-day period to cure for minor violations.

On April 14, 2021, the Commerce Committee adopted a strike-all and reported the bill favorably as a committee substitute. The committee substitute:

- Changes the effective date to July 1, 2022;
- Changes terminology of “business” to “controller”, and “service provider” to “processor”;
- Requires controllers to meet two thresholds, instead of one, to qualify as a controller;
- Increases the controller revenue threshold to $50 million gross revenues annually, from $25 million;
- Provides that the controller threshold of dealing in 50,000 or more consumers’ personal information is limited to personal information that is used for targeted advertising in conjunction with third parties or that is not covered by an exception;
- Removed the definitions of “business purpose” and “commercial purpose”;
- Clarifies the roles and contract requirements between a controller and processor;
- Clarifies who may bring a private cause of action;
- Clarifies the jurisdiction to bring claims in Florida courts;
- Clarifies the exceptions for financial institutions, healthcare entities, and personal information related to the Fair Credit Reporting Act;
- Clarifies that enforcement by the Department of Legal Affairs is under the Florida Unfair or Deceptive Trade Practices Act;
- Provides that the definition of “consumer” to exclude a person in an employment context, and “personal information” to exclude employment contact information; and
- Makes several clarifying changes to structure, format, grammar, and intent.

This analysis is drafted to the committee substitute as passed by the Commerce Committee.