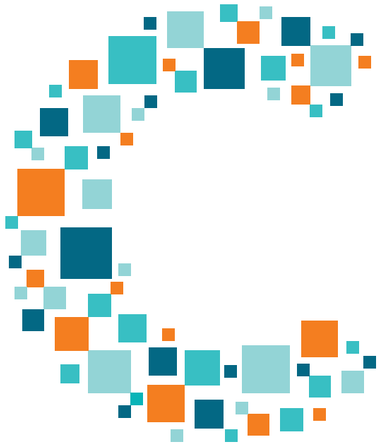
Chamber Technology Engagement Center (C_TEC)

MAJOR 2021 PRIVACY BILLS



_TEC

U.S. Chamber of Commerce
Technology Engagement Center

For more information, please contact:

Jordan Crenshaw | *Vice President*
Chamber Technology Engagement Center
JCrenshaw@uschamber.com

		S. 1494, (Moran, "Consumer Data Privacy and Security Act of 2021")	S. 2499, (Wicker, "Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act" or "SAFE DATA Act")	H.R. 1816, (Delbene, "Information Transparency and Personal Data Control Act")
Definitions	**Covered Entity**	Any entity that: i. alone, or jointly with others, determines the purpose and means of collecting or processing personal data; and ii. is—under FTC Act Section 5(2)(a) authority, common carrier under the 1934 Communications Act, or non-profit organizations	Any person that: i. is subject to the FTC Act or common carrier described in 15 U.S.C. 45(a)(2), or non-profits; ii. collects, processes, or transfers covered data; AND iii. determines the purposes and means of such collection, processing, or transfer.	"Controller" means a person that, on its own or jointly with other entities, determines the purposes and means of processing sensitive personal information.
	Covered Information	"Personal data" means information that identifies or is linked or reasonably linkable to a specific individual. "Linked or reasonably linkable" means data that can be used on its own or in combination with other information held by, or readily accessible to, the covered entity or service provider to identify the individual. This includes persistent identifiers like IP addresses, serial numbers, cookies, and unique device identifiers. Excluded are de-identified data, unreadable or undecipherable data, employee data, publicly available data, or pseudonymous data.	The term "covered data" means information that identifies or is linked ore reasonably linkable to an individual or a device that is linked or reasonably linkable to an individual. "Linked or reasonably linkable" if as a practical matter, information can be used on its own or in combination with other information held by, or readily accessible to, the covered entity, to identify such individual or such device. Excluded are aggregated data, de-identified data, employee data, and publicly available data.	Sensitive and non-sensitive personal information. No definition for non-sensitive.
	Sensitive Information	"Personal data" that is: i. A unique, government-issued identifier, such as a social security number, passport number, driver's license number, or a taxpayer identification number ii. A username or email address in combination with a password or security question and answer that would permit access to an online account iii. Biometric information iv. Content of a wire communication, oral communication, or electronic communication defined in 18 U.S.C. 2510 v. Info that relates to the past, present, or future diagnosed physical or mental health or condition of an individual; the provision of heath care to an individual; or the past, present, or future payment for the provision of health care to an individual vi. Financial account number, debit card number, credit card number, if combined with an access code, password, or credentials that provide access to such an account vii. Race or ethnic identity viii. Religious beliefs or affiliation ix. Sexual orientation x. Precise geolocation xi. Data that could cause reasonably foreseeable harm as determined by FTC rulemaking	Covered data that is: i. A unique, government-issued identifier, such as a Social Security number, passport number, or driver's license number, that is not required to be displayed to the public ii. Any covered data that describes or reveals that diagnosis or treatment of the past, present, or future physical health, mental health, or disability of an individual iii. A financial account number, debit card number, credit card number, or any required security access code, password, or credentials allowing access to any such account iv. Biometric Information v. A persistent identifier vi. Precise geolocation information vii. The contents of an individual's private communications, such as emails, texts, direct messages, or mail, or the identity of the parties subject to such communications, unless the covered entity is the intended recipient of the communication viii. Account log-in credentials such as a user name or email address, in combination with a password or security question and answer that would permit access to an online account ix. Covered data revealing an individual's racial or ethnic origin, or religion in a manner inconsistent with the individual's reasonable expectation regarding the processing or transfer of such information x. Covered data revealing the sexual orientation or sexual behavior of an individual in a manner inconsistent with the individual's reasonable expectation regarding the processing or transfer of such information xi. Covered data about the online activities of an individual that addresses or reveals a category of sensitive data described in the Act xii. Covered data that is calendar information, address book information, phone or text logs, photos, or videos maintained for private use on an individual's device xiii. Any covered data collected or processed by a covered data for the purpose of identifying sensitive covered data described in the Act xiv. Any other category of covered data designated by FTC rulemaking	Information relating to an identified or identifiable individual. That is: i. Financial account numbers ii. Health information iii. Genetic data iv. Any information pertaining to children under 13 years of age v. Social Security numbers vi. Unique government identifiers vii. Authentication credentials for a financial account, such as a username and password viii. Precise geolocation information ix. Content of a personal wire communication, oral communication, or electronic communication such as e-mail or direct messaging with respect to any entity that is not the intended recipient of the communication x. Call detail records for calls conducted in a personal and not a business capacity xi. Biometric information xii. Sexual orientation, gender identity, or intersex status xiii. Citizenship or immigration status xiv. Mental or physical health diagnosis xv. Religious beliefs xvi. Web browsing history, application usage history, and the functional equivalent of either that is data described in this subparagraph that is not aggregated data EXCEPTIONS include de-identified information, information related to employment, business-to-business information, and publicly available information.

		S. 1494, (Moran, "Consumer Data Privacy and Security Act of 2021")	S. 2499, (Wicker, "Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act" or "SAFE DATA Act")	H.R. 1816, (Delbene, "Information Transparency and Personal Data Control Act")
Obligations, Consumer Rights and Prohibitions	**Transparency**	Yes	Yes	Yes
	Access	Yes	Yes	No
	Correction	Yes	Yes	No
	Deletion	Yes	Yes	No
	Portability	Yes	Yes	No
	Fiduciary Duty	No	No	No
	AI Specific or Right to Human Review of Automated Decision Making	No	A.I. transparency reports required.	No
	Reasonable Basis	Yes	No	The regulations promulgated with regard to opt-in consent shall not apply to the processing, transmission, storage, selling, sharing, or collection of sensitive personal information in which such processing does not deviate from purposes consistent with a controller's relationship with users as understood by the reasonable use.
	Opt-In	Processing of personal data without consent or permissible purpose. No required of third parties if notice provide by first-party company. Consent can be inferred. Affirmative express consent required for processing of sensitive personal data.	Processing of and transferring of sensitive covered data to third party.	Controllers must obtain user's affirmative, express consent to any functionality that involves the sale, sharing, or other disclosure of sensitive personal information, including sharing sensitive personal information with third parties, if the sensitive personal information is to be used by the third party for purposes other than purposes outlined in the act's required privacy notice.
	Opt Out	N/A	Covered entities shall provide an individual with the ability to opt out of the collection, processing, or transfer of such covered individual's covered data before such collection, processing, or transfer occurs.	Users must be provided with the ability to opt out of the collection, transmission, storage, processing, selling, sharing, or other use of non-sensitive personal information at any time.
	Misc. Prohibited Practices	N/A	N/A	N/A

		S. 1494, (Moran, "Consumer Data Privacy and Security Act of 2021")	S. 2499, (Wicker, "Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act" or "SAFE DATA Act")	H.R. 1816, (Delbene, "Information Transparency and Personal Data Control Act")
Obligations, Consumer Rights and Prohibitions *(continued)*	**Data Minimization**	Must conduct impact assessments for material changes in processing.	Covered entities shall not collect, process, or transfer data beyond: i. What is reasonably necessary, proportionated, and limited to provide or improve a product, service, or a communication about a product or service, including what is reasonably necessary, proportionated, and limited to provide a product or service specifically requested by an individual or reasonably anticipated within the context of the covered entity's ongoing relationship with an individual; ii. What is reasonably necessary, proportionated, or limited to otherwise process or transfer covered data in a manner that is described in the privacy policy that the covered entity is required to publish under the Act; iii. What is expressly permitted by this Act or federal law. The FTC is required within one year to develop best practices for minimization.	N/A
	Discrimination	No	A covered entity, service provider, or third party may not collect, process, or transfer covered data in violation of Federal civil rights laws.	N/A
	Pricing and Service Differences	No	No denial of products or services to an individual because individual has exercised access, correction, or portability rights.	No
Accountability	**Privacy Program**	Yes	Yes	No
	Audit Requirement	Large data holders required to have privacy impact assessment.	Large data holders required to have privacy impact assessments.	Yes
	Privacy/ Security Officer Requirement	Both	Both	No
Security	**Data Security**	Covered entities and service providers shall develop, document, implement, and maintain a comprehensive data security program that contains reasonable administrative, technical, and physical safeguards designed to protect the security, confidentiality, and integrity or personal data from unauthorized access, use, destruction, acquisition, modification, or disclosure.	Covered entities must establish, implement, and maintain reasonable administrative, technical, and physical data security policies and practices to protect against risk to the confidentiality, security, and integrity of covered data.	No

		S. 1494, (Moran, "Consumer Data Privacy and Security Act of 2021")	S. 2499, (Wicker, "Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act" or "SAFE DATA Act")	H.R. 1816, (Delbene, "Information Transparency and Personal Data Control Act")
Misc. Industries	**Service Providers and Processors**	Covered entities shall only disclose personal data to a service provider pursuant to a contract that is binding on both parties and meets the following requirements: • Service providers only collect or process personal data as directed by covered entity; establish purposes for collecting and processing personal data, and a reasonable representation from service provider establishing appropriate procedures and controls • Controllers required to have due diligence of service providers • Service providers required to assist covered entities as practicable for control requests • Service providers required to delete data after performance • Service providers required to provide written representation of compliance	• Service providers shall not process service provider data for any processing purpose not performed on behalf of, and at the direction of, the covered entity that transferred the data to the service provider; shall not transfer service provider data to a third party for any purpose other than a purpose performed on behalf of, or at the direction of, the covered entity that transferred the data to the service provider without the affirmative express consent of the individual to whom the service provider data relates • Service providers required to delete or deidentify service provider data as practicable after completion of service or service period • Service providers exempted from access, correction, portability, deletion requirements but shall help covered entity comply as practicable upon receiving notice from the covered entity • Service providers are exempted from opt-in for sensitive data and covered entity data minimization requirements. • Due diligence required by covered entities for service providers FTC required to provide guidance within 2 years for service provider relationship issues.	• The documented instructions form a controller to a processor or third party shall adhere to the limits of the consent granted under the Act's opt-in requirements, and processors and third parties shall not use or disclose the sensitive personal information for any purposes or in any way that exceeds the limits of the required consent. • Controllers shall honor an opt out request and communicate the request to processors or third parties it has shared data with. Processors and third parties receiving the opt out requests to the extent of their role in the collection, transmission, storage, processing, selling, sharing, or other use of non-sensitive personal information. • Processing by a processor must be governed by a contract between the controller and the processor that is binding on both parties and that sets the processor to processes the personal data only on documented instructions from the controller. Processors shall share sensitive personal information with a subcontractor only for purposes of providing services and only after first providing the controller with an opportunity to object. • Controllers and processors not liable for failures of other processors.
	Data Brokers	No	Registration with FTC	No
	Small Business Relief	Accuracy, Correction, and Access requests not required for small businesses and compliance for other misc. requirements takes into whether a small business. A small business is a covered entity or service provider that in the last six months did not employ more than 500 employees and did not maintain $50 million or more in average gross receipts over the last three years. Additionally to be considered a small business, an entity cannot collect or process annually the personal data of 1 million or more individuals OR the sensitive personal data of 100,000 or more individuals.	Covered entities noted required to comply with access, correction, deletion, and portability requests, data minimization requirements or have privacy/security officers if: i. the covered entity's average annual gross revenues did not exceed $50 million; ii. on average, the covered entity annual processed the covered data of less than 1 million individuals; iii. the covered entity never employed more than 500 individuals at any one time; AND iv. the covered entity derived less than 50 percent of its revenues from transferring covered data.	Small businesses, controllers who collect, store, process, sell, share, or otherwise use sensitive personal information relating to 250,000 or fewer individuals per year, are exempted from the audit requirement.
	Children's Privacy	No	No	Expands children's data for those under 13 to opt-in

		S. 1494, (Moran, "Consumer Data Privacy and Security Act of 2021")	S. 2499, (Wicker, "Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act" or "SAFE DATA Act")	H.R. 1816, (Delbene, "Information Transparency and Personal Data Control Act")
Enforcement Issues and Effective Date	**Enforcement Agency**	FTC	FTC	FTC with expanded funding and staff
	Safe Harbor	N/A	FTC–approved certification programs enabled deemed compliance	No
	Expanded Penalty Authority	Civil Penalty	No	No
	State AG Enforcement	Yes	Yes	Yes
	Rulemaking	Yes	Yes	Yes
	Private Right of Action	No	No	No
	Effective Date	1 year after enactment but preemption kicks in immediately.	18 months after enactment	180 days after enactment
	Preemption	The Act shall supersede any provision of a law, rule, regulation, or other requirement of any State or political subdivision of a State to the extent that such provision relates to the privacy or security of personal data except for data breach, rules of civil procedure, general standards of fraud and public safety, student privacy, GLBA entities, HIPAA entities, and employment, and discrimination.	No State or political subdivision of a State may adopt, maintain, enforce, or continue in effect any law, regulation, rule, requirement, or standard related to the data privacy or security and associated activity of covered entities.	No State or political subdivision of a State may adopt, maintain, enforce, or continue in effect any law, regulation, rule, requirement, or standard related to the data privacy or associated activities of covered entities. EXCEPTIONS include data breach notification, biometric, wiretapping, and public records laws.