NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

			Focal Document:	Texas Consumer Data Protection Act (CDPA)
Reference Document :	Secure Controls Framework (SCF) version 2025.2		Focal Document URL:	https://capitol.texas.gov/tlodocs/88R/billtext/html/HB00004F.htm
STRM Guidance:	https://securecontrolsframework.com/set-theory-relationship-mapping-strm/		Published STRM URL:	https://securecontrolsframework.com/content/strm/scf-strm-us-state-tx-cdpa.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
541.001	Definitions	See law for full content	Functional	subset of	Standardized Terminology	SEA-02.1	Mechanisms exist to standardize technology and process terminology to reduce confusion amongst groups and departments.	10	
541.002	Applicability of Chapter	See law for full content	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.003	Certain Information Exempt From Chapter	See law for full content	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.004	Inapplicability of Chapter	This chapter does not apply to the processing of personal data by a person in the course of a purely personal or household activity.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.005	Effect of Compliance With Parental Consent Requirements Under Certain Federal Law	A controller or processor that complies with the verifiable parental consent requirements of the Children's Online Privacy Protection Act of 1998 (15 U.S.C. Section 6501 et seq.) with respect to data collected online is considered to be in compliance with any requirement to obtain parental consent under this chapter.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.051(a)	Consumer's Personal Data Rights; Request To Exercise Rights	A consumer is entitled to exercise the consumer rights authorized by this section at any time by submitting a request to a controller specifying the consumer rights the consumer wishes to exercise. With respect to the processing of personal data belonging to a known child, a parent or legal guardian of the child may exercise the consumer rights on behalf of the child.	Functional	intersects with	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	5	
541.051(b)	Consumer's Personal Data Rights; Request To Exercise Rights	A controller shall comply with an authenticated consumer request to exercise the right to:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.051(b)(1)	Consumer's Personal Data Rights; Request To Exercise Rights	confirm whether a controller is processing the consumer's personal data and to access the personal data;	Functional	intersects with	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to complaints, concerns or questions from authenticated data subjects about how the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes of their Personal Data (PD).	5	
541.051(b)(2)	Consumer's Personal Data Rights; Request To Exercise Rights	correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data;	Functional	intersects with	Correcting Inaccurate Personal Data	PRI-06.1	Mechanisms exist to establish and implement a process for: (1) Data subjects to have inaccurate Personal Data (PD) maintained by the organization corrected or amended; and (2) Disseminating corrections or amendments of PD to other authorized users of the PD.	5	
541.051(b)(3)	Consumer's Personal Data Rights; Request To Exercise Rights	delete personal data provided by or obtained about the consumer;	Functional	intersects with	Right to Erasure	PRI-06.5	Mechanisms exist to maintain a process to erase a data subject's Personal Data (PD), in accordance with applicable laws, regulations and contractual obligations pertaining to the retention of their PD.	5	
541.051(b)(4)	Consumer's Personal Data Rights; Request To Exercise Rights	if the data is available in a digital format, obtain a copy of the consumer's personal data that the consumer previously provided to the controller in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance; or	Functional	intersects with	Personal Data (PD) Exports	PRI-06.7	Mechanisms exist to export a data subject's available Personal Data (PD) in a readily usable format, upon an authenticated request.	5	
541.051(b)(5)	Consumer's Personal Data Rights; Request To Exercise Rights	opt out of the processing of the personal data for purposes of:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.051(b)(5)(A)	Consumer's Personal Data Rights; Request To Exercise Rights	targeted advertising;	Functional	intersects with	Active Participation By Data Subjects	PRI-03.7	Mechanisms exist to compel data subjects to select the level of consent deemed appropriate by the data subject for the relevant business purpose (e.g., opt-in, opt-out, accept all cookies, etc.).	5	
541.051(b)(5)(B)	Consumer's Personal Data Rights; Request To Exercise Rights	the sale of personal data; or	Functional	intersects with	Active Participation By Data Subjects	PRI-03.7	Mechanisms exist to compel data subjects to select the level of consent deemed appropriate by the data subject for the relevant business purpose (e.g., opt-in, opt-out, accept all cookies, etc.).	5	
541.051(b)(5)(C)	Consumer's Personal Data Rights; Request To Exercise Rights	profiling in furtherance of a decision that produces a legal or similarly significant effect concerning the consumer.	Functional	intersects with	Active Participation By Data Subjects	PRI-03.7	Mechanisms exist to compel data subjects to select the level of consent deemed appropriate by the data subject for the relevant business purpose (e.g., opt-in, opt-out, accept all cookies, etc.).	5	
541.052(a)	Controller Response to Consumer Request	Except as otherwise provided by this chapter, a controller shall comply with a request submitted by a consumer to exercise the consumer's rights pursuant to Section 541.051 as provided by this section.	Functional	intersects with	Continued Use of Personal Data (PD)	PRI-03.9	Mechanisms exist to govern the continued use of Personal Data (PD) as it is collected, received, processed, stored, transmitted and/or shared until: (1) Disposal of PD occurs when there is no longer a legitimate business purpose; (2) Disposal of PD occurs when the data retention timeline for the use case is met; and/or (3) Continued use of PD is prohibited upon withdrawal of data subject consent.	5	
541.052(b)	Controller Response to Consumer Request	A controller shall respond to the consumer request without undue delay, which may not be later than the 45th day after the date of receipt of the request. The controller may extend the response period once by an additional 45 days when reasonably necessary, taking into account the complexity and number of the consumer's requests, so long as the controller informs the consumer of the extension within the initial 45-day response period, together with the reason for the extension.	Functional	intersects with	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to complaints, concerns or questions from authenticated data subjects about how the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes of their Personal Data (PD).	5	
541.052(c)	Controller Response to Consumer Request	If a controller declines to take action regarding the consumer's request, the controller shall inform the consumer without undue delay, which may not be later than the 45th day after the date of receipt of the request, of the justification for declining to take action and provide instructions on how to appeal the decision in accordance with Section 541.053.	Functional	intersects with	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to complaints, concerns or questions from authenticated data subjects about how the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes of their Personal Data (PD).	5	
541.052(d)	Controller Response to Consumer Request	A controller shall provide information in response to a consumer request free of charge, at least twice annually per consumer. If a request from a consumer is manifestly unfounded, excessive, or repetitive, the controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request or may decline to act on the request. The controller bears the burden of demonstrating for purposes of this subsection that a request is manifestly unfounded, excessive, or repetitive.	Functional	intersects with	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to complaints, concerns or questions from authenticated data subjects about how the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes of their Personal Data (PD).	5	
541.052(e)	Controller Response to Consumer Request	If a controller is unable to authenticate the request using commercially reasonable efforts, the controller is not required to comply with a consumer request submitted under Section 541.051 and may request that the consumer provide additional information reasonably necessary to authenticate the consumer and the consumer's request.	Functional	intersects with	Reject Unauthenticated or Untrustworthy Disclosure Requests	PRI-07.4	Mechanisms exist to reject unauthenticated, or untrustworthy, disclosure requests.	5	
541.052(f)	Controller Response to Consumer Request	A controller that has obtained personal data about a consumer from a source other than the consumer is considered in compliance with a consumer's request to delete that personal data pursuant to Section 541.051(b)(3) by:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.052(f)(1)	Controller Response to Consumer Request	retaining a record of the deletion request and the minimum data necessary for the purpose of ensuring the consumer's personal data remains deleted from the business's records and not using the retained data for any other purpose under this chapter; or	Functional	subset of	Documenting Data Processing Activities	PRI-14	Mechanisms exist to document Personal Data (PD) processing activities that cover collecting, receiving, processing, storing, transmitting, updating, sharing and disposal actions with sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual requirements.	10	
541.052(f)(2)	Controller Response to Consumer Request	opting the consumer out of the processing of that personal data for any purpose other than a purpose that is exempt under the provisions of this chapter.	Functional	intersects with	Active Participation By Data Subjects	PRI-03.7	Mechanisms exist to compel data subjects to select the level of consent deemed appropriate by the data subject for the relevant business purpose (e.g., opt-in, opt-out, accept all cookies, etc.).	5	
541.052(f)(2)	Controller Response to Consumer Request	opting the consumer out of the processing of that personal data for any purpose other than a purpose that is exempt under the provisions of this chapter.	Functional	intersects with	Use of Personal Data (PD)	PRI-05.9	Mechanisms exist to restrict the usage of Personal Data (PD) to purposes for which it was: (1) Originally collected; and/or (2) Authorized by the data subject, or authorized agent.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
541.053(a)	Appeal	A controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision under Section 541.052(c).	Functional	intersects with	Appeal Adverse Decision	PRI-06.3	Mechanisms exist to maintain a process for data subjects to appeal an adverse decision.	5	
541.053(a)	Appeal	A controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision under Section 541.052(c).	Functional	intersects with	Data Controller Communications	PRI-18	Mechanisms exist to receive and process data controller communications pertaining to: (1) Receiving and responding to data subject requests; (2) Updating/correcting Personal Data (PD); (3) Accounting for disclosures of PD; and (4) Accounting for PD that is stored, processed and/or transmitted on behalf of the data controller.	5	
541.053(b)	Appeal	The appeal process must be conspicuously available and similar to the process for initiating action to exercise consumer rights by submitting a request under Section 541.051.	Functional	intersects with	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5	
541.053(c)	Appeal	A controller shall inform the consumer in writing of any action taken or not taken in response to an appeal under this section not later than the 60th day after the date of receipt of the appeal, including a written explanation of the reason or reasons for the decision.	Functional	intersects with	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to complaints, concerns or questions from authenticated data subjects about how the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes of their Personal Data (PD).	5	
541.053(d)	Appeal	If the controller denies an appeal, the controller shall provide the consumer with the online mechanism described by Section 541.152 through which the consumer may contact the attorney general to submit a complaint.	Functional	intersects with	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to complaints, concerns or questions from authenticated data subjects about how the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes of their Personal Data (PD).	5	
541.054	Waiver or Limitation of Consumer Rights Prohibited	Any provision of a contract or agreement that waives or limits in any way a consumer right described by Sections 541.051, 541.052, and 541.053 is contrary to public policy and is void and unenforceable.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.055(a)	Methods for Submitting Consumer Requests	A controller shall establish two or more secure and reliable methods to enable consumers to submit a request to exercise their consumer rights under this chapter. The methods must take into account:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.055(a)(1)	Methods for Submitting Consumer Requests	the ways in which consumers normally interact with the controller;	Functional	intersects with	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	5	
541.055(a)(1)	Methods for Submitting Consumer Requests	the ways in which consumers normally interact with the controller;	Functional	intersects with	Data Controller Communications	PRI-18	Mechanisms exist to receive and process data controller communications pertaining to: (1) Receiving and responding to data subject requests; (2) Updating/correcting Personal Data (PD); (3) Accounting for disclosures of PD; and (4) Accounting for PD that is stored, processed and/or transmitted on behalf of the data controller.	5	
541.055(a)(2)	Methods for Submitting Consumer Requests	the necessity for secure and reliable communications of those requests; and	Functional	intersects with	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to complaints, concerns or questions from authenticated data subjects about how the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes of their Personal Data (PD).	5	
541.055(a)(3)	Methods for Submitting Consumer Requests	the ability of the controller to authenticate the identity of the consumer making the request.	Functional	intersects with	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to complaints, concerns or questions from authenticated data subjects about how the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes of their Personal Data (PD).	5	
541.055(a)(3)	Methods for Submitting Consumer Requests	the ability of the controller to authenticate the identity of the consumer making the request.	Functional	intersects with	Strong Customer Authentication (SCA)	WEB-06	Mechanisms exist to implement Strong Customer Authentication (SCA) for consumers to reasonably prove their identity.	5	
541.055(b)	Methods for Submitting Consumer Requests	A controller may not require a consumer to create a new account to exercise the consumer's rights under this subchapter but may require a consumer to use an existing account.	Functional	intersects with	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to complaints, concerns or questions from authenticated data subjects about how the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes of their Personal Data (PD).	5	
541.055(c)	Methods for Submitting Consumer Requests	Except as provided by Subsection (d), if the controller maintains an Internet website, the controller must provide a mechanism on the website for consumers to submit requests for information required to be disclosed under this chapter.	Functional	intersects with	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5	
541.055(d)	Methods for Submitting Consumer Requests	A controller that operates exclusively online and has a direct relationship with a consumer from whom the controller collects personal information is only required to provide an e-mail address for the submission of requests described by Subsection (c).	Functional	intersects with	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
541.055(e)	Methods for Submitting Consumer Requests	A consumer may designate another person to serve as the consumer's authorized agent and act on the consumer's behalf to opt out of the processing of the consumer's personal data under Sections 541.051(b)(5)(A) and (B). A consumer may designate an authorized agent using a technology, including a link to an Internet website, an Internet browser setting or extension, or a global setting on an electronic device, that allows the consumer to indicate the consumer's intent to opt out of the processing. A controller shall comply with an opt-out request received from an authorized agent under this subsection if the controller is able to verify, with commercially reasonable effort, the identity of the consumer and the authorized agent's authority to act on the consumer's behalf. A controller is not required to comply with an opt-out request received from an authorized agent under this subsection if:	Functional	intersects with	Authorized Agent	PRI-03.6	Mechanisms exist to allow data subjects to authorize another person or entity, acting on the data subject's behalf, to make Personal Data (PD) processing decisions.	5	
541.055(e)(1)	Methods for Submitting Consumer Requests	the authorized agent does not communicate the request to the controller in a clear and unambiguous manner;	Functional	intersects with	Authorized Agent	PRI-03.6	Mechanisms exist to allow data subjects to authorize another person or entity, acting on the data subject's behalf, to make Personal Data (PD) processing decisions.	5	
541.055(e)(2)	Methods for Submitting Consumer Requests	the controller is not able to verify, with commercially reasonable effort, that the consumer is a resident of this state;	Functional	intersects with	Authorized Agent	PRI-03.6	Mechanisms exist to allow data subjects to authorize another person or entity, acting on the data subject's behalf, to make Personal Data (PD) processing decisions.	5	
541.055(e)(3)	Methods for Submitting Consumer Requests	the controller does not possess the ability to process the request; or	Functional	intersects with	Authorized Agent	PRI-03.6	Mechanisms exist to allow data subjects to authorize another person or entity, acting on the data subject's behalf, to make Personal Data (PD) processing decisions.	5	
541.055(e)(4)	Methods for Submitting Consumer Requests	the controller does not process similar or identical requests the controller receives from consumers for the purpose of complying with similar or identical laws or regulations of another state.	Functional	intersects with	Authorized Agent	PRI-03.6	Mechanisms exist to allow data subjects to authorize another person or entity, acting on the data subject's behalf, to make Personal Data (PD) processing decisions.	5	
541.055(f)	Methods for Submitting Consumer Requests	A technology described by Subsection (e):	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.055(f)(1)	Methods for Submitting Consumer Requests	may not unfairly disadvantage another controller;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.055(f)(2)	Methods for Submitting Consumer Requests	may not make use of a default setting, but must require the consumer to make an affirmative, freely given, and unambiguous choice to indicate the consumer's intent to opt out of any processing of a consumer's personal data; and	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.055(f)(3)	Methods for Submitting Consumer Requests	must be consumer-friendly and easy to use by the average consumer.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.101(a)	Controller Duties; Transparency	A controller:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.101(a)(1)	Controller Duties; Transparency	shall limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which that personal data is processed, as disclosed to the consumer; and	Functional	intersects with	Restrict Collection To Identified Purpose	PRI-04	Mechanisms exist to minimize the collection of Personal Data (PD) to only what is adequate, relevant and limited to the purposes identified in the data privacy notice, including protections against collecting PD from minors without appropriate parental or legal guardian consent.	5	
541.101(a)(2)	Controller Duties; Transparency	for purposes of protecting the confidentiality, integrity, and accessibility of personal data, shall establish, implement, and maintain reasonable administrative, technical, and physical data security practices that are appropriate to the volume and nature of the personal data at issue.	Functional	subset of	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	10	
541.101(b)	Controller Duties; Transparency	A controller may not:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.101(b)(1)	Controller Duties; Transparency	except as otherwise provided by this chapter, process personal data for a purpose that is neither reasonably necessary to nor compatible with the disclosed purpose for which the personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent;	Functional	intersects with	Purpose Specification	PRI-02.1	Mechanisms exist to ensure the data privacy notice identifies the purpose(s) for which Personal Data (PD) is collected, received, processed, stored, transmitted, shared.	5	
541.101(b)(1)	Controller Duties; Transparency	except as otherwise provided by this chapter, process personal data for a purpose that is neither reasonably necessary to nor compatible with the disclosed purpose for which the personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent;	Functional	intersects with	Restrict Collection To Identified Purpose	PRI-04	Mechanisms exist to minimize the collection of Personal Data (PD) to only what is adequate, relevant and limited to the purposes identified in the data privacy notice, including protections against collecting PD from minors without appropriate parental or legal guardian consent.	5	
541.101(b)(2)	Controller Duties; Transparency	process personal data in violation of state and federal laws that prohibit unlawful discrimination against consumers;	Functional	subset of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
541.101(b)(2)	Controller Duties; Transparency	process personal data in violation of state and federal laws that prohibit unlawful discrimination against consumers;	Functional	subset of	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	10	
541.101(b)(3)	Controller Duties; Transparency	discriminate against a consumer for exercising any of the consumer rights contained in this chapter, including by denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods or services to the consumer; or	Functional	intersects with	Product or Service Delivery Restrictions	PRI-03.5	Mechanisms exist to prevent discrimination against a data subject for exercising their legal rights pertaining to modifying or revoking consent, including prohibiting: (1) Refusing products and/or services; (2) Charging different rates for goods and/or services; and (3) Providing different levels of quality.	5	
541.101(b)(4)	Controller Duties; Transparency	process the sensitive data of a consumer without obtaining the consumer's consent, or, in the case of processing the sensitive data of a known child, without processing that data in accordance with the Children's Online Privacy Protection Act of 1998 (15 U.S.C. Section 6501 et seq.).	Functional	intersects with	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, processing, storage, sharing, updating and disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; (2) A means for users to decline the authorization; and (3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	5	
541.101(b)(4)	Controller Duties; Transparency	process the sensitive data of a consumer without obtaining the consumer's consent, or, in the case of processing the sensitive data of a known child, without processing that data in accordance with the Children's Online Privacy Protection Act of 1998 (15 U.S.C. Section 6501 et seq.).	Functional	intersects with	Prohibition of Selling, Processing and/or Sharing Personal Data (PD)	PRI-03.3	Mechanisms exist to prevent the sale, processing and/or sharing of Personal Data (PD) when: (1) Instructed by the data subject; or (2) The data subject is a minor, where selling and/or sharing PD is legally prohibited.	5	
541.101(c)	Controller Duties; Transparency	Subsection (b)(3) may not be construed to require a controller to provide a product or service that requires the personal data of a consumer that the controller does not collect or maintain or to prohibit a controller from offering a different price, rate, level, quality, or selection of goods or services to a consumer, including offering goods or services for no fee, if the consumer has exercised the consumer's right to opt out under Section 541.051 or the offer is related to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.	Functional	intersects with	Product or Service Delivery Restrictions	PRI-03.5	Mechanisms exist to prevent discrimination against a data subject for exercising their legal rights pertaining to modifying or revoking consent, including prohibiting: (1) Refusing products and/or services; (2) Charging different rates for goods and/or services; and (3) Providing different levels of quality.	5	
541.102(a)	Privacy Notice	A controller shall provide consumers with a reasonably accessible and clear privacy notice that includes:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.102(a)(1)	Privacy Notice	the categories of personal data processed by the controller, including, if applicable, any sensitive data processed by the controller;	Functional	intersects with	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5	
541.102(a)(1)	Privacy Notice	the categories of personal data processed by the controller, including, if applicable, any sensitive data processed by the controller;	Functional	intersects with	Personal Data Categories	PRI-05.7	Mechanisms exist to define and implement data handling and protection requirements for specific categories of sensitive Personal Data (PD).	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
541.102(a)(2)	Privacy Notice	the purpose for processing personal data;	Functional	intersects with	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5	
541.102(a)(2)	Privacy Notice	the purpose for processing personal data;	Functional	intersects with	Purpose Specification	PRI-02.1	Mechanisms exist to ensure the data privacy notice identifies the purpose(s) for which Personal Data (PD) is collected, received, processed, stored, transmitted, shared.	5	
541.102(a)(3)	Privacy Notice	how consumers may exercise their consumer rights under Subchapter B, including the process by which a consumer may appeal a controller's decision with regard to the consumer's request;	Functional	intersects with	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5	
541.102(a)(4)	Privacy Notice	if applicable, the categories of personal data that the controller shares with third parties;	Functional	intersects with	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5	
541.102(a)(5)	Privacy Notice	if applicable, the categories of third parties with whom the controller shares personal data; and	Functional	intersects with	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5	
541.102(a)(6)	Privacy Notice	a description of the methods required under Section 541.055 through which consumers can submit requests to exercise their consumer rights under this chapter.	Functional	intersects with	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5	
541.102(b)	Privacy Notice	If a controller engages in the sale of personal data that is sensitive data, the controller shall include the following notice: "NOTICE: We may sell your sensitive personal data." The notice must be posted in the same location and in the same manner as the privacy notice described by Subsection (a).	Functional	intersects with	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
541.103	Sale of Data to Third Parties and Processing Data for Targeted Advertising; Disclosure	If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall clearly and conspicuously disclose that process and the manner in which a consumer may exercise the right to opt out of that process.	Functional	intersects with	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5	
541.104(a)	Duties of Processor	A processor shall adhere to the instructions of a controller and shall assist the controller in meeting or complying with the controller's duties or requirements under this chapter, including:	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
541.104(a)(1)	Duties of Processor	assisting the controller in responding to consumer rights requests submitted under Section 541.051 by using appropriate technical and organizational measures, as reasonably practicable, taking into account the nature of processing and the information available to the processor;	Functional	intersects with	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
541.104(a)(2)	Duties of Processor	assisting the controller with regard to complying with the requirement relating to the security of processing personal data and to the notification of a breach of security of the processor's system under Chapter 521, taking into account the nature of processing and the information available to the processor; and	Functional	intersects with	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
541.104(a)(3)	Duties of Processor	providing necessary information to enable the controller to conduct and document data protection assessments under Section 541.105.	Functional	intersects with	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
541.104(b)	Duties of Processor	A contract between a controller and a processor shall govern the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract must include:	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
541.104(b)(1)	Duties of Processor	clear instructions for processing data;	Functional	intersects with	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
541.104(b)(2)	Duties of Processor	the nature and purpose of processing;	Functional	intersects with	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
541.104(b)(3)	Duties of Processor	the type of data subject to processing;	Functional	intersects with	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
541.104(b)(4)	Duties of Processor	the duration of processing;	Functional	intersects with	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
541.104(b)(5)	Duties of Processor	the rights and obligations of both parties; and	Functional	intersects with	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
541.104(b)(6)	Duties of Processor	a requirement that the processor shall:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.104(b)(6)(A)	Duties of Processor	ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data;	Functional	intersects with	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
541.104(b)(6)(B)	Duties of Processor	at the controller's direction, delete or return all personal data to the controller as requested after the provision of the service is completed, unless retention of the personal data is required by law;	Functional	intersects with	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
541.104(b)(6)(C)	Duties of Processor	make available to the controller, on reasonable request, all information in the processor's possession necessary to demonstrate the processor's compliance with the requirements of this chapter;	Functional	intersects with	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
541.104(b)(6)(D)	Duties of Processor	allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor; and	Functional	intersects with	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
541.104(b)(6)(E)	Duties of Processor	engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the requirements of the processor with respect to the personal data.	Functional	intersects with	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
541.104(c)	Duties of Processor	Notwithstanding the requirement described by Subsection (b)(6)(D), a processor, in the alternative, may arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the requirements under this chapter using an appropriate and accepted control standard or framework and assessment procedure. The processor shall provide a report of the assessment to the controller on request.	Functional	intersects with	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
541.104(d)	Duties of Processor	This section may not be construed to relieve a controller or a processor from the liabilities imposed on the controller or processor by virtue of its role in the processing relationship as described by this chapter.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.104(e)	Duties of Processor	A determination of 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 on the context in which personal data is to be processed. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains in the role of a processor.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.105(a)	Data Protection Assessments	A controller shall conduct and document a data protection assessment of each of the following processing activities involving personal data:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.105(a)(1)	Data Protection Assessments	the processing of personal data for purposes of targeted advertising;	Functional	intersects with	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
541.105(a)(2)	Data Protection Assessments	the sale of personal data;	Functional	intersects with	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
541.105(a)(3)	Data Protection Assessments	the processing of personal data for purposes of profiling, if the profiling presents a reasonably foreseeable risk of:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.105(a)(3)(A)	Data Protection Assessments	unfair or deceptive treatment of or unlawful disparate impact on consumers;	Functional	intersects with	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
541.105(a)(3)(B)	Data Protection Assessments	financial, physical, or reputational injury to consumers;	Functional	intersects with	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
541.105(a)(3)(C)	Data Protection Assessments	a physical or other intrusion on the solitude or seclusion, or the private affairs or concerns, of consumers, if the intrusion would be offensive to a reasonable person; or	Functional	intersects with	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
541.105(a)(3)(D)	Data Protection Assessments	other substantial injury to consumers;	Functional	intersects with	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
541.105(a)(4)	Data Protection Assessments	the processing of sensitive data; and	Functional	intersects with	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
541.105(a)(5)	Data Protection Assessments	any processing activities involving personal data that present a heightened risk of harm to consumers.	Functional	intersects with	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
541.105(b)	Data Protection Assessments	A data protection assessment conducted under Subsection (a) must:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.105(b)(1)	Data Protection Assessments	identify and weigh the direct or indirect benefits that may flow from the processing to the controller, the consumer, other stakeholders, and the public, against the potential risks to the rights of the consumer associated with that processing, as mitigated by safeguards that can be employed by the controller to reduce the risks; and	Functional	intersects with	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
541.105(b)(2)	Data Protection Assessments	factor into the assessment:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.105(b)(2)(A)	Data Protection Assessments	the use of deidentified data;	Functional	intersects with	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
541.105(b)(2)(B)	Data Protection Assessments	the reasonable expectations of consumers;	Functional	intersects with	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
541.105(b)(2)(C)	Data Protection Assessments	the context of the processing; and	Functional	intersects with	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
541.105(b)(2)(D)	Data Protection Assessments	the relationship between the controller and the consumer whose personal data will be processed.	Functional	intersects with	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
541.105(c)	Data Protection Assessments	A controller shall make a data protection assessment requested under Section 541.153(b) available to the attorney general pursuant to a civil investigative demand under Section 541.153.	Functional	intersects with	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
541.105(d)	Data Protection Assessments	A data protection assessment is confidential and exempt from public inspection and copying under Chapter 552, Government Code. Disclosure of a data protection assessment in compliance with a request from the attorney general does not constitute a waiver of attorney-client privilege or work product protection with respect to the assessment and any information contained in the assessment.	Functional	intersects with	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
541.105(e)	Data Protection Assessments	A single data protection assessment may address a comparable set of processing operations that include similar activities.	Functional	intersects with	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
541.105(f)	Data Protection Assessments	A data protection assessment conducted by a controller for the purpose of compliance with other laws or regulations may constitute compliance with the requirements of this section if the assessment has a reasonably comparable scope and effect.	Functional	intersects with	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
541.105(f)	Data Protection Assessments	A data protection assessment conducted by a controller for the purpose of compliance with other laws or regulations may constitute compliance with the requirements of this section if the assessment has a reasonably comparable scope and effect.	Functional	intersects with	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
541.106(a)	Deidentified or Pseudonymous Data	A controller in possession of deidentified data shall:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.106(a)(1)	Deidentified or Pseudonymous Data	take reasonable measures to ensure that the data cannot be associated with an individual;	Functional	intersects with	De-Identification (Anonymization)	DCH-23	Mechanisms exist to anonymize data by removing Personal Data (PD) from datasets.	5	
541.106(a)(2)	Deidentified or Pseudonymous Data	publicly commit to maintaining and using deidentified data without attempting to reidentify the data; and	Functional	intersects with	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5	
541.106(a)(3)	Deidentified or Pseudonymous Data	contractually obligate any recipient of the deidentified data to comply with the provisions of this chapter.	Functional	intersects with	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
541.106(b)	Deidentified or Pseudonymous Data	This chapter may not be construed to require a controller or processor to:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.106(b)(1)	Deidentified or Pseudonymous Data	reidentify deidentified data or pseudonymous data;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.106(b)(2)	Deidentified or Pseudonymous Data	maintain data in identifiable form or obtain, retain, or access any data or technology for the purpose of allowing the controller or processor to associate a consumer request with personal data; or	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.106(b)(3)	Deidentified or Pseudonymous Data	comply with an authenticated consumer rights request under Section 541.051, if the controller:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.106(b)(3)(A)	Deidentified or Pseudonymous Data	is not reasonably capable of associating the request with the personal data or it would be unreasonably burdensome for the controller to associate the request with the personal data;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.106(b)(3)(B)	Deidentified or Pseudonymous Data	does not use the personal data to recognize or respond to the specific consumer who is the subject of the personal data or associate the personal data with other personal data about the same specific consumer; and	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.106(b)(3)(C)	Deidentified or Pseudonymous Data	does not sell the personal data to any third party or otherwise voluntarily disclose the personal data to any third party other than a processor, except as otherwise permitted by this section.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.106(c)	Deidentified or Pseudonymous Data	The consumer rights under Sections 541.051(b)(1)-(4) and controller duties under Section 541.101 do not apply to pseudonymous data in cases in which the controller is able to demonstrate any information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing the information.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.106(d)	Deidentified or Pseudonymous Data	A controller that discloses pseudonymous data or deidentified data shall exercise reasonable oversight to monitor compliance with any contractual commitments to which the pseudonymous data or deidentified data is subject and shall take appropriate steps to address any breach of the contractual commitments.	Functional	intersects with	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
541.107(a)	Requirements for Small Businesses	A person described by Section 541.002(a)(3) may not engage in the sale of personal data that is sensitive data without receiving prior consent from the consumer.	Functional	intersects with	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, processing, storage, sharing, updating and disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; (2) A means for users to decline the authorization; and (3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	5	
541.107(b)	Requirements for Small Businesses	A person who violates this section is subject to the penalty under Section 541.155.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.151	Enforcement Authority Exclusive	The attorney general has exclusive authority to enforce this chapter.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.152	Internet Website and Complaint Mechanism	The attorney general shall post on the attorney general's Internet website:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.152(1)	Internet Website and Complaint Mechanism	information relating to:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.152(1)(A)	Internet Website and Complaint Mechanism	the responsibilities of a controller under Subchapters B and C;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.152(1)(B)	Internet Website and Complaint Mechanism	the responsibilities of a processor under Subchapter C; and	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.152(1)(C)	Internet Website and Complaint Mechanism	a consumer's rights under Subchapter B; and	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.152(2)	Internet Website and Complaint Mechanism	an online mechanism through which a consumer may submit a complaint under this chapter to the attorney general.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.153(a)	Investigative Authority	If the attorney general has reasonable cause to believe that a person has engaged in or is engaging in a violation of this chapter, the attorney general may issue a civil investigative demand. The procedures established for the issuance of a civil investigative demand under Section 15.10 apply to the same extent and manner to the issuance of a civil investigative demand under this section.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.153(b)	Investigative Authority	The attorney general may request, pursuant to a civil investigative demand issued under Subsection (a), that a controller disclose any data protection assessment that is relevant to an investigation conducted by the attorney general. The attorney general may evaluate the data protection assessment for compliance with the requirements set forth in Sections 541.101, 541.102, and 541.103.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.154	Notice of Violation of Chapter; Opportunity to Cure	Before bringing an action under Section 541.155, the attorney general shall notify a person in writing, not later than the 30th day before bringing the action, identifying the specific provisions of this chapter the attorney general alleges have been or are being violated. The attorney general may not bring an action against the person if:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.154(1)	Notice of Violation of Chapter; Opportunity to Cure	within the 30-day period, the person cures the identified violation; and	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.154(2)	Notice of Violation of Chapter; Opportunity to Cure	the person provides the attorney general a written statement that the person:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.154(2)(A)	Notice of Violation of Chapter; Opportunity to Cure	cured the alleged violation;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.154(2)(B)	Notice of Violation of Chapter; Opportunity to Cure	notified the consumer that the consumer's privacy violation was addressed, if the consumer's contact information has been made available to the person;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.154(2)(C)	Notice of Violation of Chapter; Opportunity to Cure	provided supportive documentation to show how the privacy violation was cured; and	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.154(2)(D)	Notice of Violation of Chapter; Opportunity to Cure	made changes to internal policies, if necessary, to ensure that no such further violations will occur.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.155(a)	Civil Penalty; Injunction	A person who violates this chapter following the cure period described by Section 541.154 or who breaches a written statement provided to the attorney general under that section is liable for a civil penalty in an amount not to exceed $7,500 for each violation.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.155(b)	Civil Penalty; Injunction	The attorney general may bring an action in the name of this state to:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.155(b)(1)	Civil Penalty; Injunction	recover a civil penalty under this section;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.155(b)(2)	Civil Penalty; Injunction	restrain or enjoin the person from violating this chapter; or	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.155(b)(3)	Civil Penalty; Injunction	recover the civil penalty and seek injunctive relief.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.155(c)	Civil Penalty; Injunction	The attorney general may recover reasonable attorney's fees and other reasonable expenses incurred in investigating and bringing an action under this section.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.155(d)	Civil Penalty; Injunction	The attorney general shall deposit a civil penalty collected under this section in accordance with Section 402.007, Government Code.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.156	No Private Right of Action	This chapter may not be construed as providing a basis for, or being subject to, a private right of action for a violation of this chapter or any other law.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.201(a)	Construction of Chapter	This chapter may not be construed to restrict a controller's or processor's ability to:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.201(a)(1)	Construction of Chapter	comply with federal, state, or local laws, rules, or regulations;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.201(a)(2)	Construction of Chapter	comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other governmental authorities;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.201(a)(2)	Construction of Chapter	comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other governmental authorities;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.201(a)(3)	Construction of Chapter	investigate, establish, exercise, prepare for, or defend legal claims;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.201(a)(4)	Construction of Chapter	provide a product or service specifically requested by a consumer or the parent or guardian of a child, perform a contract to which the consumer is a party, including fulfilling the terms of a written warranty, or take steps at the request of the consumer before entering into a contract;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.201(a)(5)	Construction of Chapter	take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or of another individual and in which the processing cannot be manifestly based on another legal basis;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.201(a)(6)	Construction of Chapter	prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.201(a)(7)	Construction of Chapter	preserve the integrity or security of systems or investigate, report, or prosecute those responsible for breaches of system security;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.201(a)(8)	Construction of Chapter	engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board or similar independent oversight entity that determines:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.201(a)(8)(A)	Construction of Chapter	if the deletion of the information is likely to provide substantial benefits that do not exclusively accrue to the controller;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.201(a)(8)(B)	Construction of Chapter	whether the expected benefits of the research outweigh the privacy risks; and	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.201(a)(8)(C)	Construction of Chapter	if the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with reidentification; or	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.201(a)(9)	Construction of Chapter	assist another controller, processor, or third party with any of the requirements under this subsection.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.201(b)	Construction of Chapter	This chapter may not be construed to prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under the laws of this state as part of a privileged communication.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
541.201(c)	Construction of Chapter	This chapter may not be construed as imposing a requirement on controllers and processors that adversely affects the rights or freedoms of any person, including the right of free speech.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.201(d)	Construction of Chapter	This chapter may not be construed as requiring a controller, processor, third party, or consumer to disclose a trade secret.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.202(a)	Collection, Use, or Retention of Data for Certain Purposes	The requirements imposed on controllers and processors under this chapter may not restrict a controller's or processor's ability to collect, use, or retain data to:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.202(a)(1)	Collection, Use, or Retention of Data for Certain Purposes	conduct internal research to develop, improve, or repair products, services, or technology;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.202(a)(2)	Collection, Use, or Retention of Data for Certain Purposes	effect a product recall;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.202(a)(3)	Collection, Use, or Retention of Data for Certain Purposes	identify and repair technical errors that impair existing or intended functionality; or	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.202(a)(4)	Collection, Use, or Retention of Data for Certain Purposes	perform internal operations that:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.202(a)(4)(A)	Collection, Use, or Retention of Data for Certain Purposes	are reasonably aligned with the expectations of the consumer;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.202(a)(4)(B)	Collection, Use, or Retention of Data for Certain Purposes	are reasonably anticipated based on the consumer's existing relationship with the controller; or	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.202(a)(4)(C)	Collection, Use, or Retention of Data for Certain Purposes	are otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.202(b)	Collection, Use, or Retention of Data for Certain Purposes	A requirement imposed on a controller or processor under this chapter does not apply if compliance with the requirement by the controller or processor, as applicable, would violate an evidentiary privilege under the laws of this state.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.203(a)	Disclosure of Personal Data to Third-Party Controller or Processor	A controller or processor that discloses personal data to a third-party controller or processor, in compliance with the requirements of this chapter, does not violate this chapter if the third-party controller or processor that receives and processes that personal data is in violation of this chapter, provided that, at the time of the data's disclosure, the disclosing controller or processor did not have actual knowledge that the recipient intended to commit a violation.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.203(b)	Disclosure of Personal Data to Third-Party Controller or Processor	A third-party controller or processor receiving personal data from a controller or processor in compliance with the requirements of this chapter does not violate this chapter for the transgressions of the controller or processor from which the third-party controller or processor receives the personal data.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.204(a)	Processing of Certain Personal Data by Controller or Other Person	Personal data processed by a controller under this subchapter may not be processed for any purpose other than a purpose listed in this subchapter unless otherwise allowed by this chapter. Personal data processed by a controller under this subchapter may be processed to the extent that the processing of the data is:	Functional	intersects with	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, updating and/or sharing Personal Data (PD) to: (1) The purpose(s) originally collected, consistent with the data privacy notice(s); (2) What is authorized by the data subject, or authorized agent; and (3) What is consistent with applicable laws, regulations and contractual obligations.	5	
541.204(a)(1)	Processing of Certain Personal Data by Controller or Other Person	reasonably necessary and proportionate to the purposes listed in this subchapter; and	Functional	intersects with	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, updating and/or sharing Personal Data (PD) to: (1) The purpose(s) originally collected, consistent with the data privacy notice(s); (2) What is authorized by the data subject, or authorized agent; and (3) What is consistent with applicable laws, regulations and contractual obligations.	5	
541.204(a)(2)	Processing of Certain Personal Data by Controller or Other Person	adequate, relevant, and limited to what is necessary in relation to the specific purposes listed in this subchapter.	Functional	intersects with	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, updating and/or sharing Personal Data (PD) to: (1) The purpose(s) originally collected, consistent with the data privacy notice(s); (2) What is authorized by the data subject, or authorized agent; and (3) What is consistent with applicable laws, regulations and contractual obligations.	5	
541.204(b)	Processing of Certain Personal Data by Controller or Other Person	Personal data collected, used, or retained under Section 541.202(a) must, where applicable, take into account the nature and purpose of such collection, use, or retention. The personal data described by this subsection is subject to reasonable administrative, technical, and physical measures to protect the confidentiality, integrity, and accessibility of the personal data and to reduce reasonably foreseeable risks of harm to consumers relating to the collection, use, or retention of personal data.	Functional	intersects with	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, updating and/or sharing Personal Data (PD) to: (1) The purpose(s) originally collected, consistent with the data privacy notice(s); (2) What is authorized by the data subject, or authorized agent; and (3) What is consistent with applicable laws, regulations and contractual obligations.	5	
541.204(c)	Processing of Certain Personal Data by Controller or Other Person	A controller that processes personal data under an exemption in this subchapter bears the burden of demonstrating that the processing of the personal data qualifies for the exemption and complies with the requirements of Subsections (a) and (b).	Functional	subset of	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	10	
541.204(d)	Processing of Certain Personal Data by Controller or Other Person	The processing of personal data by an entity for the purposes described by Section 541.201 does not solely make the entity a controller with respect to the processing of the data.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.
541.205	Local Preemption	This chapter supersedes and preempts any ordinance, resolution, rule, or other regulation adopted by a political subdivision regarding the processing of personal data by a controller or processor.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	No requirements to map to.