

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

Reference document: Secure Controls Framework (SCF) version 2026.1

STRM Guidance: <https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/>

Focal Document:

Focal Document URL:

Published STRM URL:

Oregon Consumer Information Protection Act (ORS 646A) (2025)

https://www.oregonlegislature.gov/bills_laws/ors/ors646a.html<https://content.securecontrolsframework.com/strm/scf-strm-usa-state-or-646a-2025.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	Notes
646A.570	Definitions	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
646A.572	Scope and application; exclusions	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
646A.574	Consumer requests for personal data; requirement to correct inaccuracies; requirement to delete personal data; conditions under which consumer may opt out of personal data processing; format for providing copy of personal data to consumer	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
646A.574(1)	Consumer requests for personal data; requirement to correct inaccuracies; requirement to delete personal data; conditions under which consumer may opt out of personal data processing; format for providing copy of personal data to consumer	Subject to ORS 646A.576, a consumer may:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
646A.574(1)(a)	Consumer requests for personal data; requirement to correct inaccuracies; requirement to delete personal data; conditions under which consumer may opt out of personal data processing; format for providing copy of personal data to consumer	Obtain from a controller:	Functional	Subset Of	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/or 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.	10	
646A.574(1)(a)(A)	Consumer requests for personal data; requirement to correct inaccuracies; requirement to delete personal data; conditions under which consumer may opt out of personal data processing; format for providing copy of personal data to consumer	Confirmation as to whether the controller is processing or has processed the consumer's personal data and the categories of personal data the controller is processing or has processed:	Functional	Subset Of	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/or 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.	10	
646A.574(1)(a)(B)	Consumer requests for personal data; requirement to correct inaccuracies; requirement to delete personal data; conditions under which consumer may opt out of personal data processing; format for providing copy of personal data to consumer	At the controller's option, a list of specific third parties, other than natural persons, to which the controller has disclosed:	Functional	Subset Of	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/or 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.	10	
646A.574(1)(a)(B)(i)	Consumer requests for personal data; requirement to correct inaccuracies; requirement to delete personal data; conditions under which consumer may opt out of personal data processing; format for providing copy of personal data to consumer	The consumer's personal data; or	Functional	Subset Of	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/or 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.	10	
646A.574(1)(a)(B)(ii)	Consumer requests for personal data; requirement to correct inaccuracies; requirement to delete personal data; conditions under which consumer may opt out of personal data processing; format for providing copy of personal data to consumer	Any personal data; and	Functional	Subset Of	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/or 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.	10	
646A.574(1)(a)(C)	Consumer requests for personal data; requirement to correct inaccuracies; requirement to delete personal data; conditions under which consumer may opt out of personal data processing; format for providing copy of personal data to consumer	A copy of all of the consumer's personal data that the controller has processed or is processing;	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	
646A.574(1)(b)	Consumer requests for personal data; requirement to correct inaccuracies; requirement to delete personal data; conditions under which consumer may opt out of personal data processing; format for providing copy of personal data to consumer	Require a controller to correct inaccuracies in personal data about the consumer, taking into account the nature of the personal data and the controller's purpose for processing the personal data.	Functional	Intersects With	Correcting Inaccurate Personal Data (PD)	PRI-06.1	Mechanisms exist to maintain 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	
646A.574(1)(c)	Consumer requests for personal data; requirement to correct inaccuracies; requirement to delete personal data; conditions under which consumer may opt out of personal data processing; format for providing copy of personal data to consumer	Require a controller to delete personal data about the consumer, including personal data the consumer provided to the controller, personal data the controller obtained from another source and derived data; or	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	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
646A.574(1)(d)	Consumer requests for personal data; requirement to correct inaccuracies; requirement to delete personal data; conditions under which consumer may opt out of personal data processing; format for providing copy of personal data to consumer	Opt out from a controller's processing of personal data of the consumer that the controller processes for any of the following purposes:	Functional	Subset Of	Notice of Right To Opt-Out	PRI-21	Mechanisms exist to include a notification to data subjects within the data privacy notice of(1) Their right to direct an organization that sells or shares their Personal Data (PD) to stop selling or sharing their PD; and(2) The methods available to exercise that right.	10	
646A.574(1)(d)(A)	Consumer requests for personal data; requirement to correct inaccuracies; requirement to delete personal data; conditions under which consumer may opt out of personal data processing; format for providing copy of personal data to consumer	Targeted advertising;	Functional	Subset Of	Notice of Right To Opt-Out	PRI-21	Mechanisms exist to include a notification to data subjects within the data privacy notice of(1) Their right to direct an organization that sells or shares their Personal Data (PD) to stop selling or sharing their PD; and(2) The methods available to exercise that right.	10	
646A.574(1)(d)(B)	Consumer requests for personal data; requirement to correct inaccuracies; requirement to delete personal data; conditions under which consumer may opt out of personal data processing; format for providing copy of personal data to consumer	Selling the personal data; or	Functional	Subset Of	Notice of Right To Opt-Out	PRI-21	Mechanisms exist to include a notification to data subjects within the data privacy notice of(1) Their right to direct an organization that sells or shares their Personal Data (PD) to stop selling or sharing their PD; and(2) The methods available to exercise that right.	10	
646A.574(1)(d)(C)	Consumer requests for personal data; requirement to correct inaccuracies; requirement to delete personal data; conditions under which consumer may opt out of personal data processing; format for providing copy of personal data to consumer	Profiling the consumer in furtherance of decisions that produce legal effects or effects of similar significance.	Functional	Subset Of	Notice of Right To Opt-Out	PRI-21	Mechanisms exist to include a notification to data subjects within the data privacy notice of(1) Their right to direct an organization that sells or shares their Personal Data (PD) to stop selling or sharing their PD; and(2) The methods available to exercise that right.	10	
646A.574(2)	Consumer requests for personal data; requirement to correct inaccuracies; requirement to delete personal data; conditions under which consumer may opt out of personal data processing; format for providing copy of personal data to consumer	A controller that provides a copy of personal data to a consumer under subsection (1)(a)(C) of this section shall provide the personal data in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the personal data to another person without hindrance.	Functional	Intersects With	Data Portability	PRI-06.6	Mechanisms exist to format exports of Personal Data (PD) in a structured, machine-readable format that allows data subjects to transfer their PD to another controller without hindrance.	5	
646A.574(3)	Consumer requests for personal data; requirement to correct inaccuracies; requirement to delete personal data; conditions under which consumer may opt out of personal data processing; format for providing copy of personal data to consumer	This section does not require a controller to disclose the controller's trade secrets, as defined in ORS 646.461. [2023 c.369 §3]	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
646A.575	N/A	[2011 c.393 §1; renumbered 646A.820 in 2023]	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
646A.576	Method for requesting personal data; persons who may request personal data on consumer's behalf; designation by consumer; duties of controller; process for appealing controller's refusal of consumer request	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
646A.576(1)	Method for requesting personal data; persons who may request personal data on consumer's behalf; designation by consumer; duties of controller; process for appealing controller's refusal of consumer request	A consumer may exercise the rights described in ORS 646A.574 by submitting a request to a controller using the method that the controller specifies in the privacy notice described in ORS 646A.578.	Functional	Subset Of	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/or 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.	10	
646A.576(2)	Method for requesting personal data; persons who may request personal data on consumer's behalf; designation by consumer; duties of controller; process for appealing controller's refusal of consumer request	A controller may not require a consumer to create an account for the purpose described in subsection (1) of this section, but the controller may require the consumer to use an account the consumer created previously.	Functional	Intersects With	Data Subject Authentication	PRI-06.8	Mechanisms exist to utilize reasonable consumer expectations to verify a data subject's identity, prior to taking action to disclose, share, correct, amend and/or delete Personal Data (PD).	5	
646A.576(3)	Method for requesting personal data; persons who may request personal data on consumer's behalf; designation by consumer; duties of controller; process for appealing controller's refusal of consumer request	A parent or legal guardian may exercise the rights described in ORS 646A.574 on behalf of the parent's child or on behalf of a child for whom the guardian has legal responsibility. A guardian or conservator may exercise the rights described in subsection (1) of this section on behalf of a consumer that is subject to a guardianship, conservatorship or other protective arrangement.	Functional	Subset Of	Authorized Agent	PRI-03.6	Mechanisms exist to allow data subjects to authorize another person or entity (e.g., authorized agent, proxy, etc.), acting on the data subject's behalf, to make Personal Data (PD) processing decisions.	10	
646A.576(4)	Method for requesting personal data; persons who may request personal data on consumer's behalf; designation by consumer; duties of controller; process for appealing controller's refusal of consumer request	A consumer may designate another person to act on the consumer's behalf as the consumer's authorized agent for the purpose of opting out of a controller's processing of the consumer's personal data, as provided in ORS 646A.574 (1)(d). The consumer may designate an authorized agent by means of an internet link, browser setting, browser extension, global device setting or other technology that enables the consumer to opt out of the controller's processing of the consumer's personal data. A controller shall comply with an opt-out request the controller receives from an authorized agent if the controller can verify, with commercially reasonable effort, the identity of the consumer and the authorized agent's authority to act on the consumer's behalf.	Functional	Subset Of	Authorized Agent	PRI-03.6	Mechanisms exist to allow data subjects to authorize another person or entity (e.g., authorized agent, proxy, etc.), acting on the data subject's behalf, to make Personal Data (PD) processing decisions.	10	
646A.576(5)	Method for requesting personal data; persons who may request personal data on consumer's behalf; designation by consumer; duties of controller; process for appealing controller's refusal of consumer request	Except as otherwise provided in ORS 646A.570 to 646A.589, in responding to a request under subsection (1) of this section, a controller shall:	Functional	Subset Of	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	10	
646A.576(5)(a)	Method for requesting personal data; persons who may request personal data on consumer's behalf; designation by consumer; duties of controller; process for appealing controller's refusal of consumer request	Respond to a request from a consumer without undue delay and not later than 45 days after receiving the request. The controller may extend the period within which the controller responds by an additional 45 days if the extension is reasonably necessary to comply with the consumer's request, taking into consideration the complexity of the request and the number of requests the consumer makes. A controller that intends to extend the period for responding shall notify the consumer within the initial 45-day response period and explain the reason for the extension.	Functional	Subset Of	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
646A.576(5)(b)	Method for requesting personal data; persons who may request personal data on consumer's behalf; designation by consumer; duties of controller; process for appealing controller's refusal of consumer request	Notify the consumer without undue delay and not later than 45 days after receiving the consumer's request if the controller declines to take action on the request. The controller in the notice shall explain the justification for not taking action and include instructions for appealing the controller's decision.	Functional	Subset Of	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	10	
646A.576(5)(c)	Method for requesting personal data; persons who may request personal data on consumer's behalf; designation by consumer; duties of controller; process for appealing controller's refusal of consumer request	Provide information the consumer requests once during any 12-month period without charge to the consumer. A controller may charge a reasonable fee to cover the administrative costs of complying with a second or subsequent request within the 12-month period, unless the purpose of the second or subsequent request is to verify that the controller corrected inaccuracies in, or deleted, the consumer's personal data in compliance with the consumer's request.	Functional	Subset Of	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	10	
646A.576(5)(d)	Method for requesting personal data; persons who may request personal data on consumer's behalf; designation by consumer; duties of controller; process for appealing controller's refusal of consumer request	Notify the consumer if the controller cannot, using commercially reasonable methods, authenticate the consumer's request without additional information from the consumer. A controller that sends a notification under this paragraph does not have to comply with the request until the consumer provides the information necessary to authenticate the request.	Functional	Subset Of	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	10	
646A.576(5)(e)	Method for requesting personal data; persons who may request personal data on consumer's behalf; designation by consumer; duties of controller; process for appealing controller's refusal of consumer request	Comply with a request under ORS 646A.574 (1)(d) to opt out of the controller's processing of the consumer's personal data without requiring authentication, except that:	Functional	Subset Of	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	10	
646A.576(5)(e)(A)	Method for requesting personal data; persons who may request personal data on consumer's behalf; designation by consumer; duties of controller; process for appealing controller's refusal of consumer request	controller may ask for additional information necessary to comply with the request, such as information that is necessary to identify the consumer that requested to opt out.	Functional	Subset Of	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	10	
646A.576(5)(e)(B)	Method for requesting personal data; persons who may request personal data on consumer's behalf; designation by consumer; duties of controller; process for appealing controller's refusal of consumer request	A controller may deny a request to opt out if the controller has a good-faith, reasonable and documented belief that the request is fraudulent. If the controller denies a request under this subparagraph, the controller shall notify the consumer that the controller believes the request is fraudulent, stating in the notice that the controller will not comply with the request.	Functional	Subset Of	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	10	
646A.576(6)	Method for requesting personal data; persons who may request personal data on consumer's behalf; designation by consumer; duties of controller; process for appealing controller's refusal of consumer request	A controller shall establish a process by means of which a consumer may appeal the controller's refusal to take action on a request under subsection (1) of this section. The controller's process must:	Functional	Subset Of	Appeal Adverse Decision	PRI-06.3	Mechanisms exist to maintain a process for data subjects to appeal an adverse decision.	10	
646A.576(6)(a)	Method for requesting personal data; persons who may request personal data on consumer's behalf; designation by consumer; duties of controller; process for appealing controller's refusal of consumer request	Allow a reasonable period of time after the consumer receives the controller's refusal within which to appeal;	Functional	Subset Of	Appeal Adverse Decision	PRI-06.3	Mechanisms exist to maintain a process for data subjects to appeal an adverse decision.	10	
646A.576(6)(b)	Method for requesting personal data; persons who may request personal data on consumer's behalf; designation by consumer; duties of controller; process for appealing controller's refusal of consumer request	Be conspicuously available to the consumer;	Functional	Subset Of	Appeal Adverse Decision	PRI-06.3	Mechanisms exist to maintain a process for data subjects to appeal an adverse decision.	10	
646A.576(6)(c)	Method for requesting personal data; persons who may request personal data on consumer's behalf; designation by consumer; duties of controller; process for appealing controller's refusal of consumer request	Be similar to the manner in which a consumer must submit a request under subsection (1) of this section; and	Functional	Subset Of	Appeal Adverse Decision	PRI-06.3	Mechanisms exist to maintain a process for data subjects to appeal an adverse decision.	10	
646A.576(6)(d)	Method for requesting personal data; persons who may request personal data on consumer's behalf; designation by consumer; duties of controller; process for appealing controller's refusal of consumer request	Require the controller to approve or deny the appeal within 45 days after the date on which the controller received the appeal and to notify the consumer in writing of the controller's decision and the reasons for the decision. If the controller denies the appeal, the notice must provide or specify information that enables the consumer to contact the Attorney General to submit a complaint.	Functional	Subset Of	Appeal Adverse Decision	PRI-06.3	Mechanisms exist to maintain a process for data subjects to appeal an adverse decision.	10	
646A.576(7)	Method for requesting personal data; persons who may request personal data on consumer's behalf; designation by consumer; duties of controller; process for appealing controller's refusal of consumer request	A controller that obtains personal data about a consumer from a source other than the consumer complies with the consumer's request to delete the personal data if the controller:	Functional	Intersects With	Revoke Consent	PRI-03.4	Mechanisms exist to allow data subjects to revoke consent to collect, receive, process, store, transmit, share and/or update their Personal Data (PD).	5	
646A.576(7)(a)	Method for requesting personal data; persons who may request personal data on consumer's behalf; designation by consumer; duties of controller; process for appealing controller's refusal of consumer request	Deletes the data but retains a record of the deletion request and a minimal amount of data necessary to ensure that the personal data remains deleted and does not use the minimal data for any other purpose; or	Functional	Subset Of	Cease Processing, Storing and/or Sharing Personal Data (PD)	PRI-03.10	Mechanisms exist to ensure the organization ceases collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) upon receiving a data subject's consent revocation.	10	
646A.576(7)(b)	Method for requesting personal data; persons who may request personal data on consumer's behalf; designation by consumer; duties of controller; process for appealing controller's refusal of consumer request	Opts the consumer out of the controller's processing of the consumer's personal data for any purpose other than a purpose that is exempt under ORS 646A.572. [2023 c.369 §4]	Functional	Subset Of	Cease Processing, Storing and/or Sharing Personal Data (PD)	PRI-03.10	Mechanisms exist to ensure the organization ceases collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) upon receiving a data subject's consent revocation.	10	
646A.577	N/A	[2011 c.393 §2; renumbered 646A.823 in 2023]	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
646A.578	Duties of controller; prohibitions; privacy notice to consumer	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
646A.578(1)	Duties of controller; prohibitions; privacy notice to consumer	A controller shall:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
646A.578(1)(a)	Duties of controller; prohibitions; privacy notice to consumer	Specify in the privacy notice described in subsection (4) of this section the express purposes for which the controller is collecting and processing personal data;	Functional	Subset Of	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/or 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.	10	
646A.578(1)(b)	Duties of controller; prohibitions; privacy notice to consumer	Limit the controller's collection of personal data to only the personal data that is adequate, relevant and reasonably necessary to serve the purposes the controller specified in paragraph (a) of this subsection;	Functional	Subset Of	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.	10	
646A.578(1)(c)	Duties of controller; prohibitions; privacy notice to consumer	Establish, implement and maintain for personal data the same safeguards described in ORS 646A.622 that are required for protecting personal information, as defined in ORS 646A.602, such that the controller's safeguards protect the confidentiality, integrity and accessibility of the personal data to the extent appropriate for the volume and nature of the personal data; and	Functional	Intersects With	Security of Personal Data (PD)	PRI-01.6	Mechanisms exist to ensure Personal Data (PD) is protected by logical and physical security safeguards that are sufficient and appropriately scoped to protect the confidentiality and integrity of the PD.	8	
646A.578(1)(c)	Duties of controller; prohibitions; privacy notice to consumer	Establish, implement and maintain for personal data the same safeguards described in ORS 646A.622 that are required for protecting personal information, as defined in ORS 646A.602, such that the controller's safeguards protect the confidentiality, integrity and accessibility of the personal data to the extent appropriate for the volume and nature of the personal data; and	Functional	Intersects With	Reasonable Data Privacy Practices	PRI-01.11	Mechanisms exist to limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of Personal Data (PD) according to reasonable consumer expectations for what is necessary and proportionate.	8	
646A.578(1)(d)	Duties of controller; prohibitions; privacy notice to consumer	Provide an effective means by which a consumer may revoke consent a consumer gave under ORS 646A.570 to 646A.589 to the controller's processing of the consumer's personal data. The means must be at least as easy as the means by which the consumer provided consent. Once the consumer revokes consent, the controller shall cease processing the personal data as soon as is practicable, but not later than 15 days after receiving the revocation.	Functional	Intersects With	Revoke Consent	PRI-03.4	Mechanisms exist to allow data subjects to revoke consent to collect, receive, process, store, transmit, share and/or update their Personal Data (PD).	5	
646A.578(2)	Duties of controller; prohibitions; privacy notice to consumer	A controller may not:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
646A.578(2)(a)	Duties of controller; prohibitions; privacy notice to consumer	Process personal data for purposes that are not reasonably necessary for and compatible with the purposes the controller specified in subsection (1)(a) of this section, unless the controller obtains the consumer's consent;	Functional	Subset Of	Reasonable Data Privacy Practices	PRI-01.11	Mechanisms exist to limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of Personal Data (PD) according to reasonable consumer expectations for what is necessary and proportionate.	10	
646A.578(2)(b)	Duties of controller; prohibitions; privacy notice to consumer	Process sensitive data about a consumer without first obtaining the consumer's consent or, if the controller knows the consumer is a child, without processing the sensitive data in accordance with the Children's Online Privacy Protection Act of 1996, 15 U.S.C. 6501 et seq, and the regulations, rules and guidance adopted under the Act, all as in effect on January 1, 2024;	Functional	Subset Of	Reasonable Data Privacy Practices	PRI-01.11	Mechanisms exist to limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of Personal Data (PD) according to reasonable consumer expectations for what is necessary and proportionate.	10	
646A.578(2)(c)	Duties of controller; prohibitions; privacy notice to consumer	Process a consumer's personal data for the purposes of targeted advertising, of profiling the consumer in furtherance of decisions that produce legal effects or effects of similar significance or of selling the consumer's personal data without the consumer's consent if the controller has actual knowledge that, or willfully disregards whether, the consumer is at least 13 years of age and not older than 15 years of age; or	Functional	Subset Of	Reasonable Data Privacy Practices	PRI-01.11	Mechanisms exist to limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of Personal Data (PD) according to reasonable consumer expectations for what is necessary and proportionate.	10	
646A.578(2)(d)	Duties of controller; prohibitions; privacy notice to consumer	Discriminate against a consumer that exercises a right provided to the consumer under ORS 646A.570 to 646A.589 by means such as denying goods or services, charging different prices or rates for goods or services or providing a different level of quality or selection of goods or services to the consumer.	Functional	Subset Of	Reasonable Data Privacy Practices	PRI-01.11	Mechanisms exist to limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of Personal Data (PD) according to reasonable consumer expectations for what is necessary and proportionate.	10	
646A.578(3)	Duties of controller; prohibitions; privacy notice to consumer	Subsections (1) and (2) of this section do not:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
646A.578(3)(a)	Duties of controller; prohibitions; privacy notice to consumer	Require a controller to provide a good or service that requires personal data from a consumer that the controller does not collect or maintain; or	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
646A.578(3)(b)	Duties of controller; prohibitions; privacy notice to consumer	Prohibit a controller from offering a different price, rate, level of quality or selection of goods or services to a consumer, including an offer for no fee or charge, in connection with a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discount or club card program.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
646A.578(4)	Duties of controller; prohibitions; privacy notice to consumer	A controller shall provide to consumers a reasonably accessible, clear and meaningful privacy notice that:	Functional	Subset Of	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/or 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.	10	
646A.578(4)(a)	Duties of controller; prohibitions; privacy notice to consumer	Lists the categories of personal data, including the categories of sensitive data, that the controller processes;	Functional	Subset Of	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/or 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.	10	
646A.578(4)(b)	Duties of controller; prohibitions; privacy notice to consumer	Describes the controller's purposes for processing the personal data;	Functional	Subset Of	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/or 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.	10	
646A.578(4)(c)	Duties of controller; prohibitions; privacy notice to consumer	Describes how a consumer may exercise the consumer's rights under ORS 646A.570 to 646A.589, including how a consumer may appeal a controller's denial of a consumer's request under ORS 646A.576;	Functional	Subset Of	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/or 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.	10	
646A.578(4)(d)	Duties of controller; prohibitions; privacy notice to consumer	Lists all categories of personal data, including the categories of sensitive data, that the controller shares with third parties;	Functional	Subset Of	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/or 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.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
646A.578(4)(e)	Duties of controller; prohibitions; privacy notice to consumer	Describes all categories of third parties with which the controller shares personal data at a level of detail that enables the consumer to understand what type of entity each third party is and, to the extent possible, how each third party may process personal data;	Functional	Subset Of	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/or 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.	10	
646A.578(4)(f)	Duties of controller; prohibitions; privacy notice to consumer	Specifies an electronic mail address or other online method by which a consumer can contact the controller that the controller actively monitors;	Functional	Subset Of	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/or 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.	10	
646A.578(4)(g)	Duties of controller; prohibitions; privacy notice to consumer	Identifies the controller, including any business name under which the controller registered with the Secretary of State and any assumed business name that the controller uses in this state;	Functional	Subset Of	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/or 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.	10	
646A.578(4)(h)	Duties of controller; prohibitions; privacy notice to consumer	Provides a clear and conspicuous description of any processing of personal data in which the controller engages for the purpose of targeted advertising or for the purpose of profiling the consumer in furtherance of decisions that produce legal effects or effects of similar significance, and a procedure by which the consumer may opt out of this type of processing; and	Functional	Subset Of	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/or 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.	10	
646A.578(4)(i)	Duties of controller; prohibitions; privacy notice to consumer	Describes the method or methods the controller has established for a consumer to submit a request under ORS 646A.276 (1).	Functional	Subset Of	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/or 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.	10	
646A.578(5)	Duties of controller; prohibitions; privacy notice to consumer	The method or methods described in subsection (4)(i) of this section for submitting a consumer's request to a controller must:	Functional	Subset Of	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/or 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.	10	
646A.578(5)(a)	Duties of controller; prohibitions; privacy notice to consumer	Take into account:	Functional	Subset Of	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/or 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.	10	
646A.578(5)(a)(A)	Duties of controller; prohibitions; privacy notice to consumer	Ways in which consumers normally interact with the controller;	Functional	Subset Of	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/or 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.	10	
646A.578(5)(a)(B)	Duties of controller; prohibitions; privacy notice to consumer	A need for security and reliability in communications related to the request; and	Functional	Subset Of	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/or 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.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
646A.578(5)(a)(C)	Duties of controller; prohibitions; privacy notice to consumer	The controller's ability to authenticate the identity of the consumer that makes the request;	Functional	Subset Of	Data Subject Empowerment	PRJ-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/or 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.	10	
646A.578(5)(b)	Duties of controller; prohibitions; privacy notice to consumer	Provide a clear and conspicuous link to a webpage where the consumer or an authorized agent may opt out from a controller's processing of the consumer's personal data as described in ORS 646A.574 (1)(d) or, solely if the controller does not have a capacity needed for linking to a webpage, provide another method the consumer can use to opt out; and	Functional	Subset Of	Data Privacy Notice	PRJ-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/or 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.	10	
646A.578(5)(c)	Duties of controller; prohibitions; privacy notice to consumer	Allow a consumer or authorized agent to send a signal to the controller that indicates the consumer's preference to opt out of the sale of personal data or targeted advertising under ORS 646A.574 (1)(k) by means of a platform, technology or mechanism that;	Functional	Subset Of	Global Privacy Control (GPC)	PRJ-03.8	Automated mechanisms exist to provide data subjects with functionality to exercise pre-selected opt-out preferences (e.g., opt-out signal).	10	
646A.578(5)(c)(A)	Duties of controller; prohibitions; privacy notice to consumer	Does not unfairly disadvantage another controller;	Functional	Subset Of	Global Privacy Control (GPC)	PRJ-03.8	Automated mechanisms exist to provide data subjects with functionality to exercise pre-selected opt-out preferences (e.g., opt-out signal).	10	
646A.578(5)(c)(B)	Duties of controller; prohibitions; privacy notice to consumer	Does not use a default setting but instead requires the consumer or authorized agent to make an affirmative, voluntary and unambiguous choice to opt out;	Functional	Subset Of	Global Privacy Control (GPC)	PRJ-03.8	Automated mechanisms exist to provide data subjects with functionality to exercise pre-selected opt-out preferences (e.g., opt-out signal).	10	
646A.578(5)(c)(C)	Duties of controller; prohibitions; privacy notice to consumer	Is consumer friendly and easy for an average consumer to use;	Functional	Subset Of	Global Privacy Control (GPC)	PRJ-03.8	Automated mechanisms exist to provide data subjects with functionality to exercise pre-selected opt-out preferences (e.g., opt-out signal).	10	
646A.578(5)(c)(D)	Duties of controller; prohibitions; privacy notice to consumer	Is as consistent as possible with similar platforms, technologies or mechanisms required under federal or state laws or regulations; and	Functional	Subset Of	Global Privacy Control (GPC)	PRJ-03.8	Automated mechanisms exist to provide data subjects with functionality to exercise pre-selected opt-out preferences (e.g., opt-out signal).	10	
646A.578(5)(c)(E)	Duties of controller; prohibitions; privacy notice to consumer	Enables the controller to accurately determine whether the consumer is a resident of this state and has made a legitimate request under ORS 646A.576 to opt out as described in ORS 646A.574 (1)(d).	Functional	Subset Of	Global Privacy Control (GPC)	PRJ-03.8	Automated mechanisms exist to provide data subjects with functionality to exercise pre-selected opt-out preferences (e.g., opt-out signal).	10	
646A.578(6)	Duties of controller; prohibitions; privacy notice to consumer	If a consumer or authorized agent uses a method described in subsection (5) of this section to opt out of a controller's processing of the consumer's personal data under ORS 646A.574 (1)(d) and the decision conflicts with a consumer's voluntary participation in a bona fide reward, club card or loyalty program or a program that provides premium features or discounts in return for the consumer's consent to the controller's processing of the consumer's personal data, the controller may either comply with the request to opt out or notify the consumer of the conflict and ask the consumer to affirm that the consumer intends to withdraw from the bona fide reward, club card or loyalty program or the program that provides premium features or discounts. If the consumer affirms that the consumer intends to withdraw, the controller shall comply with the request to opt out.	Functional	Intersects With	Choice & Consent	PRJ-03	Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or 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	
646A.580	N/A	[2011 c.393 §3; renumbered 646A.826 in 2023]	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
646A.581	Duties of processor of personal data; contract between controller and processor; liabilities of controller and processor	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
646A.581(1)	Duties of processor of personal data; contract between controller and processor; liabilities of controller and processor	A processor shall adhere to a controller's instructions and shall assist the controller in meeting the controller's obligations under ORS 646A.570 to 646A.589. In assisting the controller, the processor must:	Functional	Subset Of	Reasonable Data Privacy Practices	PRJ-01.11	Mechanisms exist to limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of Personal Data (PD) according to reasonable consumer expectations for what is necessary and proportionate.	10	
646A.581(1)(a)	Duties of processor of personal data; contract between controller and processor; liabilities of controller and processor	Enable the controller to respond to requests from consumers under ORS 646A.576 by means that take into account how the processor processes personal data and the information available to the processor and that use appropriate technical and organizational measures to the extent reasonably practicable;	Functional	Subset Of	Reasonable Data Privacy Practices	PRJ-01.11	Mechanisms exist to limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of Personal Data (PD) according to reasonable consumer expectations for what is necessary and proportionate.	10	
646A.581(1)(b)	Duties of processor of personal data; contract between controller and processor; liabilities of controller and processor	Adopt administrative, technical and physical safeguards that are reasonably designed to protect the security and confidentiality of the personal data the personal data and the information available to the processor; and	Functional	Subset Of	Reasonable Data Privacy Practices	PRJ-01.11	Mechanisms exist to limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of Personal Data (PD) according to reasonable consumer expectations for what is necessary and proportionate.	10	
646A.581(1)(c)	Duties of processor of personal data; contract between controller and processor; liabilities of controller and processor	Provide information reasonably necessary for the controller to conduct and document data protection assessments.	Functional	Subset Of	Reasonable Data Privacy Practices	PRJ-01.11	Mechanisms exist to limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of Personal Data (PD) according to reasonable consumer expectations for what is necessary and proportionate.	10	
646A.581(2)	Duties of processor of personal data; contract between controller and processor; liabilities of controller and processor	The processor shall enter into a contract with the controller that governs how the processor processes personal data on the controller's behalf. The contract must:	Functional	Intersects With	Data Privacy Requirements for Contractors & Service Providers	PRJ-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.	8	
646A.581(2)	Duties of processor of personal data; contract between controller and processor; liabilities of controller and processor	The processor shall enter into a contract with the controller that governs how the processor processes personal data on the controller's behalf. The contract must:	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	8	
646A.581(2)(a)	Duties of processor of personal data; contract between controller and processor; liabilities of controller and processor	Be valid and binding on both parties;	Functional	Subset Of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	
646A.581(2)(b)	Duties of processor of personal data; contract between controller and processor; liabilities of controller and processor	Set forth clear instructions for processing data, the nature and purpose of the processing, the type of data that is subject to processing and the duration of the processing;	Functional	Subset Of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	
646A.581(2)(c)	Duties of processor of personal data; contract between controller and processor; liabilities of controller and processor	Specify the rights and obligations of both parties with respect to the subject matter of the contract;	Functional	Subset Of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	
646A.581(2)(d)	Duties of processor of personal data; contract between controller and processor; liabilities of controller and processor	Ensure that each person that processes personal data is subject to a duty of confidentiality with respect to the personal data;	Functional	Subset Of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	
646A.581(2)(e)	Duties of processor of personal data; contract between controller and processor; liabilities of controller and processor	Require the processor to delete the personal data or return the personal data to the controller at the controller's direction or at the end of the provision of services, unless a law requires the processor to retain the personal data;	Functional	Subset Of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	
646A.581(2)(f)	Duties of processor of personal data; contract between controller and processor; liabilities of controller and processor	Require the processor to make available to the controller, at the controller's request, all information the controller needs to verify that the processor has complied with all obligations the processor has under ORS 646A.570 to 646A.589;	Functional	Subset Of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	
646A.581(2)(g)	Duties of processor of personal data; contract between controller and processor; liabilities of controller and processor	Require the processor to enter into a subcontract with a person the processor engages to assist with processing personal data on the controller's behalf and in the controller's name, to require the subcontractor to meet the processor's obligations under the processor's contract with the controller; and	Functional	Subset Of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	
646A.581(2)(h)	Duties of processor of personal data; contract between controller and processor; liabilities of controller and processor	Allow the controller, the controller's designee or a qualified and independent person the processor engages, in accordance with an appropriate and accepted control standard, framework or procedure, to assess the processor's policies and technical and organizational measures for complying with the processor's obligations under ORS 646A.570 to 646A.589, and require the processor to cooperate with the assessment and, at the controller's request, report the results of the assessment to the controller.	Functional	Subset Of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
646A.581(3)	Duties of processor of personal data; contract between controller and processor; liabilities of controller and processor	This section does not relieve a controller or processor from any liability that accrues under ORS 646A.570 to 646A.589 as a result of the controller's or processor's actions in processing personal data.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
646A.581(4)(a)	Duties of processor of personal data; contract between controller and processor; liabilities of controller and processor	For purposes of determining obligations under ORS 646A.570 to 646A.589, a person is a controller with respect to processing a set of personal data, and is subject to an action under ORS 646A.589 to punish a violation of ORS 646A.570 to 646A.589, if the person:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
646A.581(4)(a)(A)	Duties of processor of personal data; contract between controller and processor; liabilities of controller and processor	Does not need to adhere to another person's instructions to process the personal data;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
646A.581(4)(a)(B)	Duties of processor of personal data; contract between controller and processor; liabilities of controller and processor	Does not adhere to another person's instructions with respect to processing the personal data when the person is obligated to do so; or	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
646A.581(4)(a)(C)	Duties of processor of personal data; contract between controller and processor; liabilities of controller and processor	Begins at any point to determine the purposes and means for processing the personal data, alone or in concert with another person.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
646A.581(4)(b)	Duties of processor of personal data; contract between controller and processor; liabilities of controller and processor	A determination under this subsection is a fact-based determination that must take account of the context in which a set of personal data is processed.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
646A.581(4)(c)	Duties of processor of personal data; contract between controller and processor; liabilities of controller and processor	A processor that adheres to a controller's instructions with respect to a specific processing of personal data remains a processor. [2023 c.369 §6]	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
646A.582	N/A	[2011 c.393 §4; renumbered 646A.829 in 2023]	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
646A.583	Controller's use of deidentified data; exclusions	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
646A.583(1)(a)	Controller's use of deidentified data; exclusions	A controller that possesses deidentified data shall:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
646A.583(1)(a)(A)	Controller's use of deidentified data; exclusions	Take reasonable measures to ensure that the deidentified 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	
646A.583(1)(a)(B)	Controller's use of deidentified data; exclusions	Publicly commit to maintaining and using deidentified data without attempting to reidentify the deidentified 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/or 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	
646A.583(1)(a)(C)	Controller's use of deidentified data; exclusions	Enter into a contract with a recipient of the deidentified data and provide in the contract that the recipient must comply with the controller's obligations under ORS 646A.570 to 646A.589.	Functional	Intersects With	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or 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	
646A.583(1)(b)	Controller's use of deidentified data; exclusions	A controller that discloses deidentified data shall exercise reasonable oversight to monitor compliance with any contractual commitments to which the deidentified data is subject and shall take appropriate steps to address any breaches of the contractual commitments.	Functional	Intersects With	Reasonable Data Privacy Practices	PRI-01.11	Mechanisms exist to limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of Personal Data (PD) according to reasonable consumer expectations for what is necessary and proportionate.	5	
646A.583(1)(c)	Controller's use of deidentified data; exclusions	This section does not prohibit a controller from attempting to reidentify deidentified data solely for the purpose of testing the controller's methods for deidentifying data.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
646A.583(2)	Controller's use of deidentified data; exclusions	ORS 646A.570 to 646A.589 do not:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
646A.583(2)(a)	Controller's use of deidentified data; exclusions	Require a controller or processor to:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
646A.583(2)(a)(A)	Controller's use of deidentified data; exclusions	Reidentify deidentified data; or	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
646A.583(2)(a)(B)	Controller's use of deidentified data; exclusions	Associate a consumer with personal data in order to authenticate the consumer's request under ORS 646A.576 by:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
646A.583(2)(a)(B)(i)	Controller's use of deidentified data; exclusions	Maintaining data in identifiable form; or	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
646A.583(2)(a)(B)(ii)	Controller's use of deidentified data; exclusions	Collecting, retaining or accessing any particular data or technology.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
646A.583(2)(b)	Controller's use of deidentified data; exclusions	Require a controller or processor to comply with a consumer's request under ORS 646A.576 if the controller:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
646A.583(2)(b)(A)	Controller's use of deidentified data; exclusions	Cannot reasonably associate the request with personal data or if the controller's attempt to associate the request with personal data would be unreasonably burdensome.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
646A.583(2)(b)(B)	Controller's use of deidentified data; exclusions	Does not use personal data to recognize or respond to the specific consumer who is the subject of the personal data or associate the personal data with any other personal data about the specific consumer; and	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
646A.583(2)(b)(C)	Controller's use of deidentified data; exclusions	Does not sell or otherwise voluntarily disclose personal data to a third party, except as otherwise provided in this section. [2023 c.369 §7]	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
646A.585	N/A	[2011 c.393 §5; renumbered 646A.832 in 2023]	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
646A.586	Data protection assessment for processing activities with heightened risk of harm; criteria for conducting data protection assessment; provision to Attorney General; retention of records; confidentiality	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
646A.586(1)(a)	Data protection assessment for processing activities with heightened risk of harm; criteria for conducting data protection assessment; provision to Attorney General; retention of records; confidentiality	A controller shall conduct and document a data protection assessment for each of the controller's processing activities that presents a heightened risk of harm to a consumer.	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	
646A.586(1)(b)	Data protection assessment for processing activities with heightened risk of harm; criteria for conducting data protection assessment; provision to Attorney General; retention of records; confidentiality	Processing activities that present a heightened risk of harm to a consumer include:	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	
646A.586(1)(b)(A)	Data protection assessment for processing activities with heightened risk of harm; criteria for conducting data protection assessment; provision to Attorney General; retention of records; confidentiality	Processing personal data for the purpose of targeted advertising;	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
646A.586(1)(b)(B)	Data protection assessment for processing activities with heightened risk of harm; criteria for conducting data protection assessment; provision to Attorney General; retention of records; confidentiality	Processing sensitive data;	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	
646A.586(1)(b)(C)	Data protection assessment for processing activities with heightened risk of harm; criteria for conducting data protection assessment; provision to Attorney General; retention of records; confidentiality	Selling personal data; and	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	
646A.586(1)(b)(D)	Data protection assessment for processing activities with heightened risk of harm; criteria for conducting data protection assessment; provision to Attorney General; retention of records; confidentiality	Using the personal data for purposes of profiling, if the profiling presents a reasonably foreseeable risk of:	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	
646A.586(1)(b)(D)(i)	Data protection assessment for processing activities with heightened risk of harm; criteria for conducting data protection assessment; provision to Attorney General; retention of records; confidentiality	Unfair or deceptive treatment of, or unlawful disparate impact on, consumers;	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	
646A.586(1)(b)(D)(ii)	Data protection assessment for processing activities with heightened risk of harm; criteria for conducting data protection assessment; provision to Attorney General; retention of records; confidentiality	Financial, physical or reputational injury to consumers;	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	
646A.586(1)(b)(D)(iii)	Data protection assessment for processing activities with heightened risk of harm; criteria for conducting data protection assessment; provision to Attorney General; retention of records; confidentiality	Physical or other types of intrusion upon a consumer's solitude, seclusion or private affairs or concerns, if the intrusion would be offensive to a reasonable person; or	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	
646A.586(1)(b)(D)(iv)	Data protection assessment for processing activities with heightened risk of harm; criteria for conducting data protection assessment; provision to Attorney General; retention of records; confidentiality	Other substantial injury to consumers.	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	
646A.586(1)(c)	Data protection assessment for processing activities with heightened risk of harm; criteria for conducting data protection assessment; provision to Attorney General; retention of records; confidentiality	A single data protection assessment may address a comparable set of processing operations that present a similar heightened risk of harm.	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	
646A.586(2)	Data protection assessment for processing activities with heightened risk of harm; criteria for conducting data protection assessment; provision to Attorney General; retention of records; confidentiality	A data protection assessment shall identify and weigh how processing personal data may directly or indirectly benefit the controller, the consumer, other stakeholders and the public against potential risks to the consumer, taking into account how safeguards the controller employs can mitigate the risks. In conducting the assessment, the controller shall consider how deidentified data might reduce risks, the reasonable expectations of consumers, the context in which the data is processed and the relationship between the controller and the consumers whose personal data the controller will process.	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	
646A.586(3)	Data protection assessment for processing activities with heightened risk of harm; criteria for conducting data protection assessment; provision to Attorney General; retention of records; confidentiality	The Attorney General may require a controller to provide to the Attorney General any data protection assessments the controller has conducted if the data protection assessment is relevant to an investigation the Attorney General conducts under ORS 646A.589. The Attorney General may evaluate a data protection assessment for the controller's compliance with the requirements of ORS 646A.570 to 646A.589. If a data protection assessment the Attorney General obtains under this subsection includes information that is subject to attorney-client privilege or is work product that is subject to a privilege, the controller's provision of the data protection assessment does not waive the privilege.	Functional	Intersects With	Investigation Access Restrictions	CPL-05-2	Mechanisms exist to support official investigations by provisioning government investigators with "least privileges" and "least functionality" to ensure that government investigators only have access to the Technology Assets, Applications, Services and/or Data (TAASD) needed to perform the investigation.	5	
646A.586(4)	Data protection assessment for processing activities with heightened risk of harm; criteria for conducting data protection assessment; provision to Attorney General; retention of records; confidentiality	A data protection assessment that a controller conducts to comply with another applicable law or regulation satisfies the requirements of this section if the data protection assessment is reasonably similar in scope and effect to a data protection assessment conducted under this section.	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	
646A.586(5)	Data protection assessment for processing activities with heightened risk of harm; criteria for conducting data protection assessment; provision to Attorney General; retention of records; confidentiality	Requirements that apply to a data protection assessment under this section apply only to processing activities that occur on and after July 1, 2024, and are not retroactive.	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	
646A.586(6)	Data protection assessment for processing activities with heightened risk of harm; criteria for conducting data protection assessment; provision to Attorney General; retention of records; confidentiality	A controller shall retain for at least five years all data protection assessments the controller conducts under this section.	Functional	Intersects With	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	5	
646A.586(7)	Data protection assessment for processing activities with heightened risk of harm; criteria for conducting data protection assessment; provision to Attorney General; retention of records; confidentiality	A data protection assessment is confidential and is not subject to disclosure under ORS 192.311 to 192.478. [2023 c.369 §8]	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
646A.589	Investigative demand by Attorney General; representation by counsel; confidentiality of proceedings and materials; action to impose civil penalty or obtain injunction; amount of civil penalty; notice of violation; time limit on action; Attorney General's exclusive authority	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control