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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: USA - Montana Consumer Data Privacy Act (CDPA) (2025)
Focal Document URL: https://mca.legmt.gov/bills/mca/title_0300/chapter_0140/part_0280/sections_index.html
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-state-mt-cdpa-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	Legacy SCF #
30-14-2801	Short title	This part may be cited as the "Consumer Data Privacy Act".	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2802	Definitions	(see definitions section)	Functional	Intersects With	Standardized Terminology	GOV-03.2	Mechanisms exist to standardize technology and process terminology to reduce confusion amongst groups and departments.	5		SEA-02.1
30-14-2803(1)	Applicability	The provisions of this part, excluding 30-14-2811, 30-14-2818, and 30-14-2819, apply to persons that conduct business in this state or persons that produce products or services that are targeted to residents of this state and: (a) control or process the personal data of not less than 25,000 consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or (b) control or process the personal data of not less than 15,000 consumers and derive more than 25% of gross revenue from the sale of personal data.	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2803(2)	N/A	Sections 30-14-2811, 30-14-2818, and 30-14-2819 apply to persons that conduct business in this state or deliver commercial products or services that are intentionally targeted to residents of this state.	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2804(1)	Exemptions	This part does not apply to any:	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2804(1)(a)	N/A	body, authority, board, bureau, commission, district, or agency of this state or any political subdivision of this state;	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2804(1)(b)	N/A	nonprofit organization that is established to detect and prevent fraudulent acts in connection with insurance;	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2804(1)(c)	N/A	institution of higher education;	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2804(1)(d)	N/A	national securities association that is registered under 15 U.S.C. 78o-3 of the federal Securities Exchange Act of 1934, as amended;	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2804(1)(e)	N/A	state or federally chartered bank or credit union or an affiliate or subsidiary that is principally engaged in financial activities as described in 12 U.S.C. 1843(k);	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2804(1)(f)	N/A	personal data collected, processed, sold, or disclosed in accordance with, Title V of the Gramm-Leach-Bliley Act, 15 U.S.C. 6801, et seq.;	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2804(1)(g)	N/A	covered entity or business associate as defined in the privacy regulations of the federal Health Insurance Portability and Accountability Act of 1996, 45 CFR 160.103; or	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2804(1)(h)	N/A	insurer as defined in 33-1-201, an insurance producer as defined in 33-17-102, a third-party administrator of self-insurance, or an affiliate or subsidiary of an entity identified in this subsection (1)(h) that is principally engaged in financial activities as described in 12 U.S.C. 1843(k), except that this subsection (1)(h) does not apply to a person who, alone or in combination with another person, establishes and maintains a self-insurance program that does not otherwise engage in the business of entering into policies of insurance.	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2804(2)	N/A	Information and data exempt from this part include:	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2804(2)(a)	N/A	protected health information under the privacy regulations of the federal Health Insurance Portability and Accountability Act of 1996;	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2804(2)(b)	N/A	patient-identifying information for the purposes of 42 U.S.C. 290dd-2;	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2804(2)(c)	N/A	identifiable private information for the purposes of the federal policy for the protection of human subjects of 1991, 45 CFR, part 46;	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2804(2)(d)	N/A	identifiable private information that is otherwise information collected as part of human subjects research pursuant to the good clinical practice guidelines issued by the international council for harmonisation of technical requirements for pharmaceuticals for human use;	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2804(2)(e)	N/A	the protection of human subjects under 21 CFR, parts 6, 50, and 56, or personal data used or shared in research as defined in the federal Health Insurance Portability and Accountability Act of 1996, 45 CFR 164.501, that is conducted in accordance with the standards set forth in this subsection (2)(e), or other research conducted in accordance with applicable law;	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2804(2)(f)	N/A	information and documents created for the purposes of the Health Care Quality Improvement Act of 1986, 42 U.S.C. 11101, et seq.;	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2804(2)(g)	N/A	patient safety work products for the purposes of the Patient Safety and Quality Improvement Act of 2005, 42 U.S.C. 299b-21, et seq., as amended;	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2804(2)(h)	N/A	information derived from any of the health care-related information listed in this subsection (2) that is: (i) de-identified in accordance with the requirements for de-identification pursuant to the privacy regulations of the federal Health Insurance Portability and Accountability Act of 1996; or (ii) included in a limited data set as described in 45 CFR 164.514(e), to the extent that the information is used, disclosed, and maintained in a manner specified in 45 CFR 164.514(e);	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2804(2)(i)	N/A	information originating from and intermingled to be indistinguishable with or information treated in the same manner as information exempt under this subsection (2) that is maintained by a covered entity or business associate as defined in the privacy regulations of the federal Health Insurance Portability and Accountability Act of 1996, 45 CFR 160.103, or a program or qualified service organization, as specified in 42 U.S.C. 290dd-2, as amended;	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2804(2)(j)	N/A	information used for public health activities and purposes as authorized by the federal Health Insurance Portability and Accountability Act of 1996, community health activities, and population health activities;	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2804(2)(k)	N/A	the collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency, furnisher, or user that provides information for use in a consumer report and by a user of a consumer report, but only to the extent that the activity is regulated by and authorized under the Fair Credit Reporting Act, 15 U.S.C. 1681, as amended;	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2804(2)(l)	N/A	personal data collected, processed, sold, or disclosed in compliance with the Driver's Privacy Protection Act of 1994, 18 U.S.C. 2721, et seq., as amended;	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2804(2)(m)	N/A	personal data regulated by the Family Educational Rights and Privacy Act of 1974, 20 U.S.C. 1232g, et seq., as amended;	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2804(2)(n)	N/A	personal data collected, processed, sold, or disclosed in compliance with the Farm Credit Act of 1993, 12 U.S.C. 2001, et seq., as amended;	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2804(2)(o)	N/A	data processed or maintained: (i) by an individual applying to, employed by, or acting as an agent or independent contractor of a controller, processor, or third party to the extent that the data is collected and used within the context of that role; (ii) as the emergency contact information of an individual under this part and used for emergency contact purposes; or (iii) that is necessary to retain to administer benefits for another individual relating to the individual who is the subject of the information under subsection (2)(a) and is used for the purposes of administering the benefits; and	Functional	No Relationship	N/A	N/A	N/A	0		

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: USA - Montana Consumer Data Privacy Act (CDPA) (2025)
Focal Document URL: https://mca.legmt.gov/bills/mca/title_0300/chapter_0140/part_0280/sections_index.html
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-state-mt-cdpa-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	Legacy SCF #
30-14-2804(2)(p)	N/A	personal data collected, processed, sold, or disclosed in relation to price, route, or service, as these terms are used in the Airline Deregulation Act of 1978, 49 U.S.C. 40101, et seq., as amended, by an air carrier subject to the Airline Deregulation Act of 1978, to the extent this part is preempted by the Airline Deregulation Act of 1978, 49 U.S.C. 41713, as amended.	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2804(3)	N/A	Controllers and processors that comply with the verifiable parental consent requirements of the Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501, et seq., shall be considered compliant with any obligation to obtain parental consent pursuant to this part.	Functional	Intersects With	Parent or Guardian Opt-In Consent For Minors	PRI-27.1	Mechanisms exist to obtain parental or guardian consent for Personal Data (PD) processing actions through reasonable consumer expectations, when the data subject is a minor.	3		PRI-03.13
30-14-2805 through 30-14-2807	Reserved	30-14-2805 through 30-14-2807 reserved.	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2808(1)	Consumer personal data -- opt-out -- compliance -- appeals	A consumer must have the right to:	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2808(1)(a)	N/A	confirm whether a controller is processing the consumer's personal data and access the consumer's personal data, unless such confirmation or access would require the controller to reveal a trade secret;	Functional	Intersects With	Data Subject Empowerment	PRI-39.1	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.	8		PRI-06
30-14-2808(1)(b)	N/A	correct inaccuracies in the consumer's personal data, considering 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 (PD)	PRI-39.3	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.	8		PRI-06.1
30-14-2808(1)(c)	N/A	delete personal data about the consumer;	Functional	Intersects With	De-Identification (Anonymization)	DCH-36	Mechanisms exist to de-identify sensitive and/or regulated data through (1) Anonymization; (2) De-identification; (3) Pseudonymization; and/or (4) Redaction.	3		DCH-23
30-14-2808(1)(c)	N/A	delete personal data about the consumer;	Functional	Intersects With	Right to Erasure	PRI-40	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.	8		PRI-06.5
30-14-2808(1)(d)	N/A	obtain a copy of the consumer's personal data previously provided by the consumer to the controller in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the personal data to another controller without hindrance when the processing is carried out by automated means, provided the controller is not required to reveal any trade secret; and	Functional	Intersects With	Data Portability	PRI-41	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.	8		PRI-06.6
30-14-2808(1)(d)	N/A	obtain a copy of the consumer's personal data previously provided by the consumer to the controller in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the personal data to another controller without hindrance when the processing is carried out by automated means, provided the controller is not required to reveal any trade secret; and	Functional	Intersects With	Personal Data (PD) Exports	PRI-41.1	Mechanisms exist to export a data subject's available Personal Data (PD) in a readily usable format, upon an authenticated request.	8		PRI-06.7
30-14-2808(1)(e)	N/A	opt out of the processing of the consumer's personal data for the purposes of: (i) targeted advertising; (ii) the sale of the consumer's personal data, except as provided in 30-14-2812(2); or (iii) profiling in furtherance of automated decisions that produce legal or similarly significant effects concerning the consumer.	Functional	Intersects With	Tailored Consent	PRI-24.2	Mechanisms exist to allow data subjects to modify permission to collect, receive, process, store, transmit, share, update and/or dispose selected attributes of their Personal Data (PD).	8		PRI-03.1
30-14-2808(1)(e)	N/A	opt out of the processing of the consumer's personal data for the purposes of: (i) targeted advertising; (ii) the sale of the consumer's personal data, except as provided in 30-14-2812(2); or (iii) profiling in furtherance of automated decisions that produce legal or similarly significant effects concerning the consumer.	Functional	Intersects With	Prohibition of Selling, Processing and/or Sharing Personal Data (PD)	PRI-24.5	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.	8		PRI-03.3
30-14-2808(1)(e)	N/A	opt out of the processing of the consumer's personal data for the purposes of: (i) targeted advertising; (ii) the sale of the consumer's personal data, except as provided in 30-14-2812(2); or (iii) profiling in furtherance of automated decisions that produce legal or similarly significant effects concerning the consumer.	Functional	Intersects With	Automated Decision-Making Technology (ADMT) Opt-Out Consent	PRI-36.3	Mechanisms exist to provide concise, unambiguous and understandable instructions on how data subjects can opt-out of Automated Decision-Making Technology (ADMT).	5		PRI-19.2
30-14-2808(2)	N/A	A consumer may exercise rights under this section by a secure and reliable means established by the controller and described to the consumer in the controller's privacy notice.	Functional	Intersects With	Data Privacy Notice	PRI-21	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.	8		PRI-02
30-14-2808(2)	N/A	A consumer may exercise rights under this section by a secure and reliable means established by the controller and described to the consumer in the controller's privacy notice.	Functional	Intersects With	Data Subject Empowerment	PRI-39.1	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.	8		PRI-06

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: USA - Montana Consumer Data Privacy Act (CDPA) (2025)
Focal Document URL: https://mca.legmt.gov/bills/mca/title_0300/chapter_0140/part_0280/sections_index.html
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-state-mt-cdpa-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	Legacy SCF #
30-14-2808(3)(a)	N/A	A consumer may designate an authorized agent in accordance with 30-14-2809 to exercise the rights of the consumer to opt out of the processing of the consumer's personal data under subsection (1)(e) on behalf of the consumer.	Functional	Intersects With	Authorized Agent	PRI-28	Mechanisms exist to allow data subjects to authorize another person or entity (e.g., authorized agent and proxy), acting on the data subject's behalf, to make Personal Data (PD) processing decisions.	8		PRI-03.6
30-14-2808(3)(b)	N/A	A parent or legal guardian of a known child may exercise the consumer rights on the known child's behalf regarding the processing of personal data.	Functional	Intersects With	Parent or Guardian Opt-In Consent For Minors	PRI-27.1	Mechanisms exist to obtain parental or guardian consent for Personal Data (PD) processing actions through reasonable consumer expectations, when the data subject is a minor.	8		PRI-03.13
30-14-2808(3)(c)	N/A	A guardian or conservator of a consumer subject to a guardianship, conservatorship, or other protective arrangement, may exercise the rights on the consumer's behalf regarding the processing of personal data.	Functional	Intersects With	Authorized Agent	PRI-28	Mechanisms exist to allow data subjects to authorize another person or entity (e.g., authorized agent and proxy), acting on the data subject's behalf, to make Personal Data (PD) processing decisions.	8		PRI-03.6
30-14-2808(4)	N/A	Except as otherwise provided in this part, a controller shall comply with a request by a consumer to exercise the consumer rights authorized pursuant to this section as follows:	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2808(4)(a)	N/A	A controller shall respond to the consumer without undue delay, but not later than 45 days after receipt of the request. The controller may extend the response period by 45 additional days when reasonably necessary, considering the complexity and number of the consumer's requests, provided the controller informs the consumer of the extension within the initial 45-day response period and the reason for the extension.	Functional	Intersects With	Data Subject Rights Management	PRI-39	Mechanisms exist to facilitate the receipt, validation, fulfillment and documentation of data subject rights requests in accordance with applicable statutory, regulatory and/or contractual obligations.	5		PRI-06.4
30-14-2808(4)(b)	N/A	If a controller declines to act regarding the consumer's request, the controller shall inform the consumer without undue delay, but not later than 45 days after receipt of the request, of the justification for declining to act and provide instructions for how to appeal the decision.	Functional	Intersects With	Data Subject Rights Management	PRI-39	Mechanisms exist to facilitate the receipt, validation, fulfillment and documentation of data subject rights requests in accordance with applicable statutory, regulatory and/or contractual obligations.	5		PRI-06.4
30-14-2808(4)(b)	N/A	If a controller declines to act regarding the consumer's request, the controller shall inform the consumer without undue delay, but not later than 45 days after receipt of the request, of the justification for declining to act and provide instructions for how to appeal the decision.	Functional	Intersects With	Appeal Adverse Decision	PRI-39.5	Mechanisms exist to maintain a process for data subjects to appeal an adverse decision.	5		PRI-06.3
30-14-2808(4)(c)	N/A	Information provided in response to a consumer request must be provided by a controller, free of charge, once for each consumer during any 12-month period. If requests from a consumer are manifestly unfounded, excessive, technically infeasible, or repetitive, the controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request or decline to act on the request. The controller bears the burden of demonstrating the manifestly unfounded, excessive, technically infeasible, or repetitive nature of the request.	Functional	Intersects With	Data Subject Rights Management	PRI-39	Mechanisms exist to facilitate the receipt, validation, fulfillment and documentation of data subject rights requests in accordance with applicable statutory, regulatory and/or contractual obligations.	5		PRI-06.4
30-14-2808(4)(c)	N/A	Information provided in response to a consumer request must be provided by a controller, free of charge, once for each consumer during any 12-month period. If requests from a consumer are manifestly unfounded, excessive, technically infeasible, or repetitive, the controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request or decline to act on the request. The controller bears the burden of demonstrating the manifestly unfounded, excessive, technically infeasible, or repetitive nature of the request.	Functional	Intersects With	Justification To Reject Disclosure Requests	PRI-18.2	Mechanisms exist to document justifiable reasons for rejecting a data subject's access request for disclosure when the request is: (1) Harassing; (2) Repetitive; (3) Fraudulent; (4) Unjustified; and/or (5) Unlawful.	5		PRI-07.5
30-14-2808(4)(d)	N/A	If a controller is unable to authenticate a request to exercise any of the rights afforded under subsections (1)(a) through (1)(d) of this section using commercially reasonable efforts, the controller may not be required to comply with a request to initiate an action pursuant to this section and shall provide notice to the consumer that the controller is unable to authenticate the request to exercise the right or rights until the consumer provides additional information reasonably necessary to authenticate the consumer and the consumer's request to exercise the consumer's rights. A controller may not be required to authenticate an opt-out request, but a controller may deny an opt-out request if the controller has a good faith, reasonable, and documented belief that the request is fraudulent. If a controller denies an opt-out request because the controller believes the request is fraudulent, the controller shall send notice to the person who made the request disclosing that the controller believes the request is fraudulent and that the controller may not comply with the request.	Functional	Intersects With	Data Subject Rights Management	PRI-39	Mechanisms exist to facilitate the receipt, validation, fulfillment and documentation of data subject rights requests in accordance with applicable statutory, regulatory and/or contractual obligations.	5		PRI-06.4
30-14-2808(4)(d)	N/A	If a controller is unable to authenticate a request to exercise any of the rights afforded under subsections (1)(a) through (1)(d) of this section using commercially reasonable efforts, the controller may not be required to comply with a request to initiate an action pursuant to this section and shall provide notice to the consumer that the controller is unable to authenticate the request to exercise the right or rights until the consumer provides additional information reasonably necessary to authenticate the consumer and the consumer's request to exercise the consumer's rights. A controller may not be required to authenticate an opt-out request, but a controller may deny an opt-out request if the controller has a good faith, reasonable, and documented belief that the request is fraudulent. If a controller denies an opt-out request because the controller believes the request is fraudulent, the controller shall send notice to the person who made the request disclosing that the controller believes the request is fraudulent and that the controller may not comply with the request.	Functional	Intersects With	Data Subject Authentication	PRI-38	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).	8		PRI-06.8
30-14-2808(4)(d)	N/A	If a controller is unable to authenticate a request to exercise any of the rights afforded under subsections (1)(a) through (1)(d) of this section using commercially reasonable efforts, the controller may not be required to comply with a request to initiate an action pursuant to this section and shall provide notice to the consumer that the controller is unable to authenticate the request to exercise the right or rights until the consumer provides additional information reasonably necessary to authenticate the consumer and the consumer's request to exercise the consumer's rights. A controller may not be required to authenticate an opt-out request, but a controller may deny an opt-out request if the controller has a good faith, reasonable, and documented belief that the request is fraudulent. If a controller denies an opt-out request because the controller believes the request is fraudulent, the controller shall send notice to the person who made the request disclosing that the controller believes the request is fraudulent and that the controller may not comply with the request.	Functional	Intersects With	Justification To Reject Disclosure Requests	PRI-18.2	Mechanisms exist to document justifiable reasons for rejecting a data subject's access request for disclosure when the request is: (1) Harassing; (2) Repetitive; (3) Fraudulent; (4) Unjustified; and/or (5) Unlawful.	5		PRI-07.5
30-14-2808(4)(e)	N/A	A controller that has obtained personal data about a consumer from a source other than the consumer must be deemed in compliance with the consumer's request to delete the consumer's data pursuant to subsection (1)(c) by: (i) 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 controller's records and not using the retained data for any other purpose pursuant to the provisions of this part; or (ii) opting the consumer out of the processing of the consumer's personal data for any purpose except for those exempted pursuant to the provisions of this part.	Functional	Intersects With	Usage Restrictions of Personal Data (PD)	PRI-29	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating 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		PRI-05.4

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **USA - Montana Consumer Data Privacy Act (CDPA) (2025)**
Focal Document URL: https://mca.legmt.gov/bills/mca/title_0300/chapter_0140/part_0280/sections_index.html
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-state-mt-cdpa-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	Legacy SCF #
30-14-2808(4)(e)	N/A	A controller that has obtained personal data about a consumer from a source other than the consumer must be deemed in compliance with the consumer's request to delete the consumer's data pursuant to subsection (1)(c) by: (i) 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 controller's records and not using the retained data for any other purpose pursuant to the provisions of this part; or (ii) opting the consumer out of the processing of the consumer's personal data for any purpose except for those exempted pursuant to the provisions of this part.	Functional	Intersects With	Personal Data (PD) Retention & Disposal	PRI-30	Mechanisms exist to: (1) Retain Personal Data (PD), including metadata, for an organization-defined time period to fulfill the purpose(s) identified in the notice or as required by law; (2) Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage; and (3) Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records).	5		PRI-05
30-14-2808(4)(e)	N/A	A controller that has obtained personal data about a consumer from a source other than the consumer must be deemed in compliance with the consumer's request to delete the consumer's data pursuant to subsection (1)(c) by: (i) 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 controller's records and not using the retained data for any other purpose pursuant to the provisions of this part; or (ii) opting the consumer out of the processing of the consumer's personal data for any purpose except for those exempted pursuant to the provisions of this part.	Functional	Intersects With	Right to Erasure	PRI-40	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		PRI-06.5
30-14-2808(4)(e)	N/A	A controller that has obtained personal data about a consumer from a source other than the consumer must be deemed in compliance with the consumer's request to delete the consumer's data pursuant to subsection (1)(c) by: (i) 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 controller's records and not using the retained data for any other purpose pursuant to the provisions of this part; or (ii) opting the consumer out of the processing of the consumer's personal data for any purpose except for those exempted pursuant to the provisions of this part.	Functional	Intersects With	Data Subject Communications Documentation	PRI-37.2	Mechanisms exist to maintain records of data subject requests and responses in accordance with an established documentation retention schedule that adheres to applicable statutory, regulatory and/or contractual obligations.	5		PRI-17.3
30-14-2808(5)	N/A	A controller shall establish a process for a consumer to appeal the controller's refusal to act on a request within a reasonable period after the consumer's receipt of the decision. The appeal process must be conspicuously available and like the process for submitting requests to initiate action pursuant to this section. Not later than 60 days after receipt of an appeal, a controller shall inform the consumer in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If the appeal is denied, the controller shall also provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the attorney general to submit a complaint.	Functional	Intersects With	Data Subject Rights Management	PRI-39	Mechanisms exist to facilitate the receipt, validation, fulfillment and documentation of data subject rights requests in accordance with applicable statutory, regulatory and/or contractual obligations.	5		PRI-06.4
30-14-2808(5)	N/A	A controller shall establish a process for a consumer to appeal the controller's refusal to act on a request within a reasonable period after the consumer's receipt of the decision. The appeal process must be conspicuously available and like the process for submitting requests to initiate action pursuant to this section. Not later than 60 days after receipt of an appeal, a controller shall inform the consumer in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If the appeal is denied, the controller shall also provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the attorney general to submit a complaint.	Functional	Intersects With	Appeal Adverse Decision	PRI-39.5	Mechanisms exist to maintain a process for data subjects to appeal an adverse decision.	8		PRI-06.3
30-14-2808(6)	N/A	In response to a consumer request under subsection (1)(a), a controller may not disclose the following information about a consumer but shall inform the consumer instead with sufficient particularity that the controller has collected this information: (a) social security number; (b) driver's license number or other government-issued identification number; (c) financial account number; (d) health insurance account number or medical identification number; (e) account password, security questions, or answer; or (f) biometric data.	Functional	Intersects With	Data Subject Empowerment	PRI-39.1	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.	5		PRI-06
30-14-2809(1)	Authorized agent	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 for one or more of the purposes specified in 30-14-2808(1)(e). The consumer may designate an authorized agent by way of a technology, including but not limited to an internet link or a browser setting, browser extension, or global device setting indicating a customer's intent to opt out of such processing.	Functional	Intersects With	Authorized Agent	PRI-28	Mechanisms exist to allow data subjects to authorize another person or entity (e.g., authorized agent and proxy), acting on the data subject's behalf, to make Personal Data (PD) processing decisions.	8		PRI-03.6
30-14-2809(1)	Authorized agent	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 for one or more of the purposes specified in 30-14-2808(1)(e). The consumer may designate an authorized agent by way of a technology, including but not limited to an internet link or a browser setting, browser extension, or global device setting indicating a customer's intent to opt out of such processing.	Functional	Intersects With	Global Privacy Control (GPC)	PRI-26.3	Automated mechanisms exist to provide data subjects with functionality to exercise pre-selected opt-out preferences (e.g., opt-out signal).	5		PRI-03.8
30-14-2809(2)	N/A	A controller shall comply with an opt-out request received from an authorized agent 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.	Functional	Intersects With	Authorized Agent	PRI-28	Mechanisms exist to allow data subjects to authorize another person or entity (e.g., authorized agent and proxy), acting on the data subject's behalf, to make Personal Data (PD) processing decisions.	8		PRI-03.6
30-14-2809(2)	N/A	A controller shall comply with an opt-out request received from an authorized agent 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.	Functional	Intersects With	Data Subject Authentication	PRI-38	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		PRI-06.8
30-14-2809(3)	N/A	Opt-out methods must:	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2809(3)(a)	N/A	provide a clear and conspicuous link on the controller's internet website to an internet web page that enables a consumer, or an agent of the consumer, to opt out of the targeted advertising or sale of the consumer's personal data; and	Functional	Intersects With	Opt-Out Links	PRI-26.1	Mechanisms exist to publish conspicuous links for data subjects to exercise their rights to: (1) Limit the collection and/or use of Personal Data (PD); and (2) Not sell or share PD.	8		PRI-21.1
30-14-2809(3)(a)	N/A	provide a clear and conspicuous link on the controller's internet website to an internet web page that enables a consumer, or an agent of the consumer, to opt out of the targeted advertising or sale of the consumer's personal data; and	Functional	Intersects With	Alternative Opt-Out Link	PRI-26.2	Mechanisms exist to publish a single, clearly labeled link that allows data subjects to efficiently exercise opt-out rights to: (1) Limit the collection and/or use of Personal Data (PD); and (2) Prohibit the sale or sharing of PD.	5		PRI-21.2

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: USA - Montana Consumer Data Privacy Act (CDPA) (2025)
Focal Document URL: https://mca.legmt.gov/bills/mca/title_0300/chapter_0140/part_0280/sections_index.html
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-state-mt-cdpa-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	Legacy SCF #
30-14-2809(3)(b)	N/A	by no later than January 1, 2025, allow a consumer to opt out of any processing of the consumer's personal data for the purposes of targeted advertising, or any sale of such personal data through an opt-out preference signal sent with the consumer's consent, to the controller by a platform, technology, or mechanism that: (i) may not unfairly disadvantage another controller; (ii) may not make use of a default setting, but require the consumer to make an affirmative, freely given and unambiguous choice to opt out of any processing of a customer's personal data pursuant to this part; (iii) must be consumer-friendly and easy to use by the average consumer; (iv) must be consistent with any federal or state law or regulation; and (v) must allow the controller to accurately determine whether the consumer is a resident of the state and whether the consumer has made a legitimate request to opt out of any sale of a consumer's personal data or targeted advertising.	Functional	Intersects With	Global Privacy Control (GPC)	PRI-26.3	Automated mechanisms exist to provide data subjects with functionality to exercise pre-selected opt-out preferences (e.g., opt-out signal).	8		PRI-03.8
30-14-2809(3)(b)	N/A	by no later than January 1, 2025, allow a consumer to opt out of any processing of the consumer's personal data for the purposes of targeted advertising, or any sale of such personal data through an opt-out preference signal sent with the consumer's consent, to the controller by a platform, technology, or mechanism that: (i) may not unfairly disadvantage another controller; (ii) may not make use of a default setting, but require the consumer to make an affirmative, freely given and unambiguous choice to opt out of any processing of a customer's personal data pursuant to this part; (iii) must be consumer-friendly and easy to use by the average consumer; (iv) must be consistent with any federal or state law or regulation; and (v) must allow the controller to accurately determine whether the consumer is a resident of the state and whether the consumer has made a legitimate request to opt out of any sale of a consumer's personal data or targeted advertising.	Functional	Intersects With	Active Participation For Consent By Data Subjects	PRI-24.1	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 and accept all cookies).	5		PRI-03.7
30-14-2809(3)(b)	N/A	by no later than January 1, 2025, allow a consumer to opt out of any processing of the consumer's personal data for the purposes of targeted advertising, or any sale of such personal data through an opt-out preference signal sent with the consumer's consent, to the controller by a platform, technology, or mechanism that: (i) may not unfairly disadvantage another controller; (ii) may not make use of a default setting, but require the consumer to make an affirmative, freely given and unambiguous choice to opt out of any processing of a customer's personal data pursuant to this part; (iii) must be consumer-friendly and easy to use by the average consumer; (iv) must be consistent with any federal or state law or regulation; and (v) must allow the controller to accurately determine whether the consumer is a resident of the state and whether the consumer has made a legitimate request to opt out of any sale of a consumer's personal data or targeted advertising.	Functional	Intersects With	Choice Architecture	PRI-23	Mechanisms exist to avoid choice architecture that impairs, interferes with or subverts a consumer's ability to make well-informed choices.	5		PRI-02.11
30-14-2809(4)(a)	N/A	If a consumer's decision to opt out of any processing of the consumer's personal data for the purposes of targeted advertising, or any sale of personal data, through an opt-out preference signal sent in accordance with the provisions of subsection (3) conflicts with the consumer's existing controller-specific privacy setting or voluntary participation in a controller's bona fide loyalty, rewards, premium features, discounts, or club card program, the controller shall comply with the consumer's opt-out preference signal but may notify the consumer of the conflict and provide the choice to confirm controller-specific privacy settings or participation in such a program.	Functional	Intersects With	Global Privacy Control (GPC)	PRI-26.3	Automated mechanisms exist to provide data subjects with functionality to exercise pre-selected opt-out preferences (e.g., opt-out signal).	5		PRI-03.8
30-14-2809(4)(a)	N/A	If a consumer's decision to opt out of any processing of the consumer's personal data for the purposes of targeted advertising, or any sale of personal data, through an opt-out preference signal sent in accordance with the provisions of subsection (3) conflicts with the consumer's existing controller-specific privacy setting or voluntary participation in a controller's bona fide loyalty, rewards, premium features, discounts, or club card program, the controller shall comply with the consumer's opt-out preference signal but may notify the consumer of the conflict and provide the choice to confirm controller-specific privacy settings or participation in such a program.	Functional	Intersects With	Financial Incentives For Personal Data (PD)	PRI-19	Mechanisms exist to strictly govern financial incentives offered to data subjects for Personal Data (PD) to ensure compliance with applicable legal and regulatory requirements.	3		PRI-01.10
30-14-2809(4)(b)	N/A	If a controller responds to consumer opt-out requests received in accordance with subsection (3) by informing the consumer of a charge for the use of any product or service, the controller shall present the terms of any financial incentive offered pursuant to subsection (3) for the retention, use, sale, or sharing of the consumer's personal data.	Functional	Intersects With	Notice of Financial Incentive	PRI-19.1	Mechanisms exist to provide data subjects with a Notice of Financial Incentive that explains the material terms of a financial incentive, price or service difference so the data subject can make an informed decision about whether to participate.	8		PRI-17.2
30-14-2809(4)(b)	N/A	If a controller responds to consumer opt-out requests received in accordance with subsection (3) by informing the consumer of a charge for the use of any product or service, the controller shall present the terms of any financial incentive offered pursuant to subsection (3) for the retention, use, sale, or sharing of the consumer's personal data.	Functional	Intersects With	Financial Incentives For Personal Data (PD)	PRI-19	Mechanisms exist to strictly govern financial incentives offered to data subjects for Personal Data (PD) to ensure compliance with applicable legal and regulatory requirements.	5		PRI-01.10
30-14-2810	Reserved	30-14-2810 reserved.	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2811(1)(a)	Duties of controllers -- duty of care -- rebuttable presumption	A controller that offers an online service, product, or feature to a consumer whom the controller actually knows or willfully disregards is a minor shall use reasonable care to avoid a heightened risk of harm to minors caused by the online service, product, or feature.	Functional	Intersects With	Risk Assessment	RSK-13	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	3		RSK-04
30-14-2811(1)(a)	Duties of controllers -- duty of care -- rebuttable presumption	A controller that offers an online service, product, or feature to a consumer whom the controller actually knows or willfully disregards is a minor shall use reasonable care to avoid a heightened risk of harm to minors caused by the online service, product, or feature.	Functional	Intersects With	Reasonable Data Privacy Practices	PRI-09	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		PRI-01.11
30-14-2811(1)(a)	Duties of controllers -- duty of care -- rebuttable presumption	A controller that offers an online service, product, or feature to a consumer whom the controller actually knows or willfully disregards is a minor shall use reasonable care to avoid a heightened risk of harm to minors caused by the online service, product, or feature.	Functional	Intersects With	Privacy-Aware Design	PRI-04	Mechanisms exist to formally incorporate the organization's data privacy principles into engineering, product and model design requirements to ensure data privacy is built in by default and by design.	5		PRI-01.12
30-14-2811(1)(b)	N/A	In an enforcement action brought by the attorney general pursuant to 30-14-2817, there is a rebuttable presumption that a controller used reasonable care as required under this section if the controller complied with this section.	Functional	Intersects With	Ability To Demonstrate Conformity	CPL-04	Mechanisms exist to ensure the organization is able to demonstrate security, compliance and/or resilience capability conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.	3		CPL-01.3
30-14-2811(2)	N/A	Unless a controller has obtained consent in accordance with subsection (3), a controller that offers an online service, product, or feature to a consumer whom the controller actually knows or willfully disregards is a minor may not:	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2811(2)(a)	N/A	process a minor's personal data:	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2811(2)(a)(i)	N/A	for the purposes of: (A) targeted advertising; (B) the sale of personal data; or (C) profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer;	Functional	Intersects With	Prohibition of Selling, Processing and/or Sharing Personal Data (PD)	PRI-24.5	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		PRI-03.3
30-14-2811(2)(a)(i)	N/A	for the purposes of: (A) targeted advertising; (B) the sale of personal data; or (C) profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer;	Functional	Intersects With	Parent or Guardian Opt-In Consent For Minors	PRI-27.1	Mechanisms exist to obtain parental or guardian consent for Personal Data (PD) processing actions through reasonable consumer expectations, when the data subject is a minor.	5		PRI-03.13

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: USA - Montana Consumer Data Privacy Act (CDPA) (2025)
Focal Document URL: https://mca.legmt.gov/bills/mca/title_0300/chapter_0140/part_0280/sections_index.html
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-state-mt-cdpa-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	Legacy SCF #
30-14-2811(2)(a)(ii)	N/A	for any processing purpose other than the processing purpose that the controller disclosed at the time the controller collected the minor's personal data or that is reasonably necessary for and compatible with the processing purpose that the controller disclosed at the time the controller collected the minor's personal data; or	Functional	Intersects With	Usage Restrictions of Personal Data (PD)	PRI-29	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating 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		PRI-05.4
30-14-2811(2)(a)(ii)	N/A	for any processing purpose other than the processing purpose that the controller disclosed at the time the controller collected the minor's personal data or that is reasonably necessary for and compatible with the processing purpose that the controller disclosed at the time the controller collected the minor's personal data; or	Functional	Intersects With	Restrict Collection, Processing & Sharing To Identified Purpose	PRI-31.1	Mechanisms exist to minimize the collection, processing and/or sharing 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		PRI-04
30-14-2811(2)(a)(iii)	N/A	for longer than is reasonably necessary to provide the online service, product, or feature;	Functional	Intersects With	Personal Data (PD) Retention & Disposal	PRI-30	Mechanisms exist to: (1) Retain Personal Data (PD), including metadata, for an organization-defined time period to fulfill the purpose(s) identified in the notice or as required by law; (2) Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage; and (3) Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records).	5		PRI-05
30-14-2811(2)(b)	N/A	use a system design feature to significantly increase, sustain, or extend a minor's use of the online service, product, or feature; or	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2811(2)(c)	N/A	collect a minor's precise geolocation data unless: (i) the minor's precise geolocation data is reasonably necessary for the controller to provide the online service, product, or feature; (ii) the controller only collects and retains the minor's precise geolocation data for the time necessary to provide the online service, product, or feature; and (iii) the controller provides to the minor a signal indicating that the controller is collecting the minor's precise geolocation data and makes the signal available to the minor for the entire duration of the collection of the minor's precise geolocation data. This subsection (2)(c)(iii) does not apply to a service or application that is used by and under the direction of a ski area operator.	Functional	Intersects With	Real-Time or Layered Notice	PRI-21.5	Mechanisms exist to provide real-time and/or layered notice when Personal Data (PD) is collected that provides data subjects with a summary of key points or more detailed information that is specific to the organization's data privacy notice.	5		PRI-02.7
30-14-2811(2)(c)	N/A	collect a minor's precise geolocation data unless: (i) the minor's precise geolocation data is reasonably necessary for the controller to provide the online service, product, or feature; (ii) the controller only collects and retains the minor's precise geolocation data for the time necessary to provide the online service, product, or feature; and (iii) the controller provides to the minor a signal indicating that the controller is collecting the minor's precise geolocation data and makes the signal available to the minor for the entire duration of the collection of the minor's precise geolocation data. This subsection (2)(c)(iii) does not apply to a service or application that is used by and under the direction of a ski area operator.	Functional	Intersects With	Personal Data (PD) Retention & Disposal	PRI-30	Mechanisms exist to: (1) Retain Personal Data (PD), including metadata, for an organization-defined time period to fulfill the purpose(s) identified in the notice or as required by law; (2) Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage; and (3) Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records).	5		PRI-05
30-14-2811(2)(c)	N/A	collect a minor's precise geolocation data unless: (i) the minor's precise geolocation data is reasonably necessary for the controller to provide the online service, product, or feature; (ii) the controller only collects and retains the minor's precise geolocation data for the time necessary to provide the online service, product, or feature; and (iii) the controller provides to the minor a signal indicating that the controller is collecting the minor's precise geolocation data and makes the signal available to the minor for the entire duration of the collection of the minor's precise geolocation data. This subsection (2)(c)(iii) does not apply to a service or application that is used by and under the direction of a ski area operator.	Functional	Intersects With	Restrict Collection, Processing & Sharing To Identified Purpose	PRI-31.1	Mechanisms exist to minimize the collection, processing and/or sharing 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		PRI-04
30-14-2811(3)(a)	N/A	A controller may not engage in the activities described in subsection (2) unless the controller obtains: (i) the minor's consent; or (ii) if the minor is a child, the consent of the minor's parent or legal guardian. A controller that complies with the verifiable parental consent requirements established in the Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501, et seq., as amended, and the regulations, rules, guidance, and exemptions adopted pursuant to this act, as amended, is considered to have satisfied any requirement to obtain parental consent under this subsection (3)(a)(ii).	Functional	Intersects With	Data Subject Consent	PRI-24	Mechanisms exist to enable data subjects to authorize the collection, receipt, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where the data subject is provided, prior to collection, with: (1) Plain language explaining the potential data privacy risks of the authorization; (2) A means to decline the authorization; and (3) Necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	5		PRI-03
30-14-2811(3)(a)	N/A	A controller may not engage in the activities described in subsection (2) unless the controller obtains: (i) the minor's consent; or (ii) if the minor is a child, the consent of the minor's parent or legal guardian. A controller that complies with the verifiable parental consent requirements established in the Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501, et seq., as amended, and the regulations, rules, guidance, and exemptions adopted pursuant to this act, as amended, is considered to have satisfied any requirement to obtain parental consent under this subsection (3)(a)(ii).	Functional	Intersects With	Parent or Guardian Opt-In Consent For Minors	PRI-27.1	Mechanisms exist to obtain parental or guardian consent for Personal Data (PD) processing actions through reasonable consumer expectations, when the data subject is a minor.	5		PRI-03.13
30-14-2811(3)(b)(i)	N/A	A controller that offers an online service, product, or feature to a consumer whom the controller actually knows or willfully disregards is a minor may not: (A) provide a consent mechanism that is designed to substantially subvert or impair or is manipulated with the effect of substantially subverting or impairing user autonomy, decision-making, or choice; or (B) except as provided in subsection (3)(b)(ii), offer a direct messaging apparatus for use by a minor without providing readily accessible and easy-to-use safeguards to limit the ability of an adult to send unsolicited communications to the minor with whom the adult is not connected.	Functional	Intersects With	Data Subject Consent	PRI-24	Mechanisms exist to enable data subjects to authorize the collection, receipt, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where the data subject is provided, prior to collection, with: (1) Plain language explaining the potential data privacy risks of the authorization; (2) A means to decline the authorization; and (3) Necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	5		PRI-03
30-14-2811(3)(b)(i)	N/A	A controller that offers an online service, product, or feature to a consumer whom the controller actually knows or willfully disregards is a minor may not: (A) provide a consent mechanism that is designed to substantially subvert or impair or is manipulated with the effect of substantially subverting or impairing user autonomy, decision-making, or choice; or (B) except as provided in subsection (3)(b)(ii), offer a direct messaging apparatus for use by a minor without providing readily accessible and easy-to-use safeguards to limit the ability of an adult to send unsolicited communications to the minor with whom the adult is not connected.	Functional	Intersects With	Choice Architecture	PRI-23	Mechanisms exist to avoid choice architecture that impairs, interferes with or subverts a consumer's ability to make well-informed choices.	8		PRI-02.11
30-14-2811(3)(b)(ii)	N/A	Subsection (3)(b)(i)(B) does not apply to an online service, product, or feature of which the predominant or exclusive function is: (A) electronic mail; or (B) direct messaging consisting of text, photos, or videos that are sent between devices by electronic means in which messages are: (I) shared between the sender and the recipient; (II) only visible to the sender and the recipient; and (III) not posted publicly.	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2811(4)	N/A	Subsections (2)(a) and (2)(b) do not apply to a service or application that is used by and under the direction of an educational entity, including a learning management system or a student engagement program.	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2812(1)	Data processing by controller -- limitations	A controller shall:	Functional	No Relationship	N/A	N/A	N/A	0		

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: USA - Montana Consumer Data Privacy Act (CDPA) (2025)
Focal Document URL: https://mca.legmt.gov/bills/mca/title_0300/chapter_0140/part_0280/sections_index.html
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-state-mt-cdpa-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	Legacy SCF #
30-14-2812(1)(a)	N/A	limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which the personal data is processed, as disclosed to the consumer;	Functional	Intersects With	Restrict Collection, Processing & Sharing To Identified Purpose	PRI-31.1	Mechanisms exist to minimize the collection, processing and/or sharing 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		PRI-04
30-14-2812(1)(b)	N/A	establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data appropriate to the volume and nature of the personal data at issue; and	Functional	Intersects With	Security of Personal Data (PD)	PRI-10	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.	5		PRI-01.6
30-14-2812(1)(c)	N/A	provide an effective mechanism for a consumer to revoke the consumer's consent under this section that is at least as easy as the mechanism by which the consumer provided the consumer's consent and, on revocation of the consent, cease to process the personal data as soon as practicable, but not later than 45 days after the receipt of the request.	Functional	Intersects With	Revoke Consent	PRI-24.3	Mechanisms exist to allow data subjects to revoke consent to collect, receive, process, store, transmit, share and/or update their Personal Data (PD).	5		PRI-03.4
30-14-2812(1)(c)	N/A	provide an effective mechanism for a consumer to revoke the consumer's consent under this section that is at least as easy as the mechanism by which the consumer provided the consumer's consent and, on revocation of the consent, cease to process the personal data as soon as practicable, but not later than 45 days after the receipt of the request.	Functional	Intersects With	Cease Processing, Storing and/or Sharing Personal Data (PD)	PRI-29.2	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.	8		PRI-03.10
30-14-2812(2)	N/A	A controller may not:	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2812(2)(a)	N/A	except as otherwise provided in this part, process personal data for purposes that are not reasonably necessary to or compatible with the disclosed purposes for which the personal data is processed as disclosed to the consumer unless the controller obtains the consumer's consent;	Functional	Intersects With	Usage Restrictions of Personal Data (PD)	PRI-29	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating 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		PRI-05.4
30-14-2812(2)(a)	N/A	except as otherwise provided in this part, process personal data for purposes that are not reasonably necessary to or compatible with the disclosed purposes 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, Processing & Sharing To Identified Purpose	PRI-31.1	Mechanisms exist to minimize the collection, processing and/or sharing 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		PRI-04
30-14-2812(2)(b)	N/A	process sensitive data concerning a consumer without obtaining the consumer's consent or, in the case of the processing of sensitive data concerning a known child, without processing the sensitive data in accordance with the Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501, et seq.;	Functional	Intersects With	Data Subject Consent	PRI-24	Mechanisms exist to enable data subjects to authorize the collection, receipt, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where the data subject is provided, prior to collection, with: (1) Plain language explaining the potential data privacy risks of the authorization; (2) A means to decline the authorization; and (3) Necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	5		PRI-03
30-14-2812(2)(b)	N/A	process sensitive data concerning a consumer without obtaining the consumer's consent or, in the case of the processing of sensitive data concerning a known child, without processing the sensitive data in accordance with the Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501, et seq.;	Functional	Intersects With	Parent or Guardian Opt-In Consent For Minors	PRI-27.1	Mechanisms exist to obtain parental or guardian consent for Personal Data (PD) processing actions through reasonable consumer expectations, when the data subject is a minor.	5		PRI-03.13
30-14-2812(2)(c)	N/A	process personal data in violation of the laws of this state and federal laws that prohibit unlawful discrimination against consumers;	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-02	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	3		CPL-01
30-14-2812(2)(d)	N/A	process the personal data of a consumer for the purposes of targeted advertising or sell the consumer's personal data without the consumer's consent under circumstances in which a controller has actual knowledge or willfully disregards that the consumer is at least 13 years of age but younger than 16 years of age; or	Functional	Intersects With	Prohibition of Selling, Processing and/or Sharing Personal Data (PD)	PRI-24.5	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		PRI-03.3
30-14-2812(2)(d)	N/A	process the personal data of a consumer for the purposes of targeted advertising or sell the consumer's personal data without the consumer's consent under circumstances in which a controller has actual knowledge or willfully disregards that the consumer is at least 13 years of age but younger than 16 years of age; or	Functional	Intersects With	Parent or Guardian Opt-In Consent For Minors	PRI-27.1	Mechanisms exist to obtain parental or guardian consent for Personal Data (PD) processing actions through reasonable consumer expectations, when the data subject is a minor.	5		PRI-03.13
30-14-2812(2)(e)	N/A	discriminate against a consumer for exercising any of the consumer rights contained in this part, including 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.	Functional	Intersects With	Product or Service Delivery Restrictions	PRI-13	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		PRI-03.5
30-14-2812(3)	N/A	Nothing in subsection (1) or (2) may 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 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 their right to opt out pursuant to this part or the offering is in connection with a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2812(4)	N/A	If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall clearly and conspicuously disclose the processing in its privacy notice and provide access to a clear and conspicuous method outside the privacy notice for a consumer to opt out of the sale or processing. This method may include but is not limited to an internet hyperlink clearly labeled "your opt-out rights" or "your privacy rights" that directly effectuates the opt-out request or takes consumers to a web page where the consumer can make the opt-out request.	Functional	Intersects With	Data Privacy Notice	PRI-21	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.	8		PRI-02
30-14-2812(4)	N/A	If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall clearly and conspicuously disclose the processing in its privacy notice and provide access to a clear and conspicuous method outside the privacy notice for a consumer to opt out of the sale or processing. This method may include but is not limited to an internet hyperlink clearly labeled "your opt-out rights" or "your privacy rights" that directly effectuates the opt-out request or takes consumers to a web page where the consumer can make the opt-out request.	Functional	Intersects With	Data Subject Right To Opt-Out	PRI-26	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.	5		PRI-21

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **USA - Montana Consumer Data Privacy Act (CDPA) (2025)**
Focal Document URL: https://mca.legmt.gov/bills/mca/title_0300/chapter_0140/part_0280/sections_index.html
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-state-mt-cdpa-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	Legacy SCF #
30-14-2812(4)	N/A	If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall clearly and conspicuously disclose the processing in its privacy notice and provide access to a clear and conspicuous method outside the privacy notice for a consumer to opt out of the sale or processing. This method may include but is not limited to an internet hyperlink clearly labeled "your opt-out rights" or "your privacy rights" that directly effectuates the opt-out request or takes consumers to a web page where the consumer can make the opt-out request.	Functional	Intersects With	Opt-Out Links	PRI-26.1	Mechanisms exist to publish conspicuous links for data subjects to exercise their rights to: (1) Limit the collection and/or use of Personal Data (PD); and (2) Not sell or share PD.	8		PRI-21.1
30-14-2812(4)	N/A	If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall clearly and conspicuously disclose the processing in its privacy notice and provide access to a clear and conspicuous method outside the privacy notice for a consumer to opt out of the sale or processing. This method may include but is not limited to an internet hyperlink clearly labeled "your opt-out rights" or "your privacy rights" that directly effectuates the opt-out request or takes consumers to a web page where the consumer can make the opt-out request.	Functional	Intersects With	Alternative Opt-Out Link	PRI-26.2	Mechanisms exist to publish a single, clearly labeled link that allows data subjects to efficiently exercise opt-out rights to: (1) Limit the collection and/or use of Personal Data (PD); and (2) Prohibit the sale or sharing of PD.	5		PRI-21.2
30-14-2812(5)	N/A	A controller shall provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes:	Functional	Intersects With	Data Privacy Notice	PRI-21	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.	8		PRI-02
30-14-2812(5)(a)	N/A	the categories of personal data processed by the controller;	Functional	Intersects With	Personal Data (PD) Categories	PRI-06	Mechanisms exist to define and implement data handling and protection requirements for specific categories of sensitive Personal Data (PD).	8		PRI-05.7
30-14-2812(5)(b)	N/A	the purpose for processing personal data;	Functional	Intersects With	Purpose Specification	PRI-22	Mechanisms exist to ensure data privacy notices identify the purpose(s) for which Personal Data (PD) is collected, received, processed, stored, transmitted and/or shared.	5		PRI-02.1
30-14-2812(5)(c)	N/A	the categories of personal data that the controller sells to or shares with third parties, if any;	Functional	Intersects With	Personal Data (PD) Categories	PRI-06	Mechanisms exist to define and implement data handling and protection requirements for specific categories of sensitive Personal Data (PD).	3		PRI-05.7
30-14-2812(5)(c)	N/A	the categories of personal data that the controller sells to or shares with third parties, if any;	Functional	Intersects With	Information Sharing With Third Parties	PRI-16	Mechanisms exist to disclose Personal Data (PD) to third-parties only for the purposes identified in the data privacy notice and with the implicit or explicit consent of the data subject.	5		PRI-07
30-14-2812(5)(c)	N/A	the categories of personal data that the controller sells to or shares with third parties, if any;	Functional	Intersects With	Data Privacy Notice	PRI-21	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		PRI-02
30-14-2812(5)(d)	N/A	the categories of third parties, if any, with which the controller sells or shares personal data; and	Functional	Intersects With	Information Sharing With Third Parties	PRI-16	Mechanisms exist to disclose Personal Data (PD) to third-parties only for the purposes identified in the data privacy notice and with the implicit or explicit consent of the data subject.	5		PRI-07
30-14-2812(5)(d)	N/A	the categories of third parties, if any, with which the controller sells or shares personal data; and	Functional	Intersects With	Data Privacy Notice	PRI-21	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		PRI-02
30-14-2812(5)(e)	N/A	an active e-mail address or other mechanism that the consumer may use to contact the controller;	Functional	Subset Of	Data Privacy Notice	PRI-21	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		PRI-02

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: USA - Montana Consumer Data Privacy Act (CDPA) (2025)
Focal Document URL: https://mca.legmt.gov/bills/mca/title_0300/chapter_0140/part_0280/sections_index.html
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-state-mt-cdpa-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	Legacy SCF #
30-14-2812(5)(f)	N/A	an explanation of the rights provided by 30-14-2808(1) and how consumers may exercise their consumer rights, including how a consumer may appeal a controller's decision regarding the consumer's request; and	Functional	Subset Of	Data Privacy Notice	PRI-21	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		PRI-02
30-14-2812(5)(f)	N/A	an explanation of the rights provided by 30-14-2808(1) and how consumers may exercise their consumer rights, including how a consumer may appeal a controller's decision regarding the consumer's request; and	Functional	Intersects With	Data Subject Right To Opt-Out	PRI-26	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.	5		PRI-21
30-14-2812(5)(g)	N/A	the date the privacy notice was last updated.	Functional	Subset Of	Data Privacy Notice	PRI-21	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		PRI-02
30-14-2812(6)	N/A	The privacy notice must be made available to the public in each language in which the controller provides a product or service that is subject to the privacy notice or carries out activities related to the product or service.	Functional	Intersects With	Privacy Notice Formatting	PRI-21.1	Mechanisms exist to reasonably accommodate data privacy notice formatting for consumers requiring alternative formatting due to accessibility needs through: (1) Screen resolution / screen sizes; (2) Multilingual support; and/or (3) Disability-specific concessions.	5		PRI-02.9
30-14-2812(7)	N/A	The controller shall provide the privacy notice in a manner that is reasonably accessible to and usable by individuals with disabilities.	Functional	Intersects With	Privacy Notice Formatting	PRI-21.1	Mechanisms exist to reasonably accommodate data privacy notice formatting for consumers requiring alternative formatting due to accessibility needs through: (1) Screen resolution / screen sizes; (2) Multilingual support; and/or (3) Disability-specific concessions.	5		PRI-02.9
30-14-2812(8)	N/A	Whenever a controller makes a material change to the controller's privacy notice or practices, the controller shall notify consumers affected by the material change with respect to any prospectively collected personal data and provide a reasonable opportunity for consumers to withdraw consent to any further materially different collection, processing, or transfer of previously collected personal data under the changed policy. The controller shall take all reasonable electronic measures to provide notification regarding material changes to affected consumers, taking into account available technology and the nature of the relationship.	Functional	Subset Of	Data Privacy Notice	PRI-21	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		PRI-02
30-14-2812(8)	N/A	Whenever a controller makes a material change to the controller's privacy notice or practices, the controller shall notify consumers affected by the material change with respect to any prospectively collected personal data and provide a reasonable opportunity for consumers to withdraw consent to any further materially different collection, processing, or transfer of previously collected personal data under the changed policy. The controller shall take all reasonable electronic measures to provide notification regarding material changes to affected consumers, taking into account available technology and the nature of the relationship.	Functional	Intersects With	Just-In-Time Notice & Updated Consent	PRI-24.4	Mechanisms exist to present data subjects with a new or updated consent request to collect, receive, process, store, transmit, share, update and/or dispose Personal Data (PD) in conjunction with the data action, when: (1) The original circumstances under which an individual gave consent have changed; or (2) A significant amount of time has passed since an individual gave consent.	8		PRI-03.2
30-14-2812(9)	N/A	A controller is not required to provide a separate Montana-specific privacy notice or section of a privacy notice if the controller's general privacy notice contains all of the information required by this section.	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2812(10)	N/A	The privacy notice must be posted online through a conspicuous hyperlink using the word "privacy" on the controller's website homepage or on a mobile device's application store page or download page. A controller that maintains an application on a mobile device or other device shall also include a hyperlink to the privacy notice in the application's settings menu or in a similarly conspicuous and accessible location. A controller that does not operate a website shall make the privacy notice conspicuously available to consumers through a medium regularly used by the controller to interact with consumers, including but not limited to mail.	Functional	Intersects With	Conspicuous Link To Data Privacy Notice	PRI-21.2	Mechanisms exist to include a conspicuous link to the organization's data privacy notice on all consumer-facing websites and mobile applications.	5		PRI-17.1
30-14-2812(10)	N/A	The privacy notice must be posted online through a conspicuous hyperlink using the word "privacy" on the controller's website homepage or on a mobile device's application store page or download page. A controller that maintains an application on a mobile device or other device shall also include a hyperlink to the privacy notice in the application's settings menu or in a similarly conspicuous and accessible location. A controller that does not operate a website shall make the privacy notice conspicuously available to consumers through a medium regularly used by the controller to interact with consumers, including but not limited to mail.	Functional	Intersects With	Alternative Means To Deliver Privacy Notice	PRI-21.3	Mechanisms exist to provide data subjects with a data privacy notice through alternative means for interactions that do not utilize an interface on a website or application.	5		PRI-02.14
30-14-2812(11)(a)	N/A	A controller shall establish and describe in a privacy notice one or more secure and reliable means for consumers to submit a request to exercise their consumer rights pursuant to this part considering the ways in which consumers normally interact with the controller, the need for secure and reliable communication of consumer requests, and the ability of the controller to verify the identity of the consumer making the request.	Functional	Intersects With	Data Subject Rights Management	PRI-39	Mechanisms exist to facilitate the receipt, validation, fulfillment and documentation of data subject rights requests in accordance with applicable statutory, regulatory and/or contractual obligations.	5		PRI-06.4

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: USA - Montana Consumer Data Privacy Act (CDPA) (2025)
Focal Document URL: https://mca.legmt.gov/bills/mca/title_0300/chapter_0140/part_0280/sections_index.html
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-state-mt-cdpa-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	Legacy SCF #
30-14-2812(11)(a)	N/A	A controller shall establish and describe in a privacy notice one or more secure and reliable means for consumers to submit a request to exercise their consumer rights pursuant to this part considering the ways in which consumers normally interact with the controller, the need for secure and reliable communication of consumer requests, and the ability of the controller to verify the identity of the consumer making the request.	Functional	Intersects With	Data Subject Empowerment	PRI-39.1	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.	5		PRI-06
30-14-2812(11)(b)	N/A	A controller may not require a consumer to create a new account to exercise consumer rights but may require a consumer to use an existing account.	Functional	Intersects With	Data Subject Empowerment	PRI-39.1	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.	5		PRI-06
30-14-2813(1)	Data processor -- allowances -- limitations	A processor shall adhere to the instructions of a controller and shall assist the controller in meeting the controller's obligations under this part to include:	Functional	Subset Of	Data Privacy Requirements for Contractors & Service Providers	PRI-14	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.	10		PRI-07.1
30-14-2813(1)(a)	N/A	considering the nature of processing and the information available to the processor by appropriate technical and organizational measures as much as reasonably practicable to fulfill the controller's obligation to respond to consumer rights requests;	Functional	Intersects With	Data Controller Communications	PRI-44	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.	8		PRI-18
30-14-2813(1)(a)	N/A	considering the nature of processing and the information available to the processor by appropriate technical and organizational measures as much as reasonably practicable to fulfill the controller's obligation to respond to consumer rights requests;	Functional	Intersects With	Data Subject Rights Management	PRI-39	Mechanisms exist to facilitate the receipt, validation, fulfillment and documentation of data subject rights requests in accordance with applicable statutory, regulatory and/or contractual obligations.	5		PRI-06.4
30-14-2813(1)(a)	N/A	considering the nature of processing and the information available to the processor by appropriate technical and organizational measures as much as reasonably practicable to fulfill the controller's obligation to respond to consumer rights requests;	Functional	Intersects With	Data Privacy Requirements for Contractors & Service Providers	PRI-14	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		PRI-07.1
30-14-2813(1)(b)	N/A	considering the nature of processing and the information available to the processor by assisting the controller in meeting the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a breach of security, as provided for in 30-14-1704, of the system of the processor to meet the controller's obligations; and	Functional	Intersects With	Security of Personal Data (PD)	PRI-10	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.	5		PRI-01.6
30-14-2813(1)(b)	N/A	considering the nature of processing and the information available to the processor by assisting the controller in meeting the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a breach of security, as provided for in 30-14-1704, of the system of the processor to meet the controller's obligations; and	Functional	Intersects With	Data Breach	IRO-22	Mechanisms exist to address data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations.	5		IRO-04.1
30-14-2813(1)(b)	N/A	considering the nature of processing and the information available to the processor by assisting the controller in meeting the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a breach of security, as provided for in 30-14-1704, of the system of the processor to meet the controller's obligations; and	Functional	Intersects With	Security Compromise Notification Agreements	TPM-21.1	Mechanisms exist to compel External Service Providers (ESPs) to provide notification of actual or potential compromises in the supply chain that can potentially affect or have adversely affected Technology Assets, Applications and/or Services (TAAS) that the organization utilizes.	5		TPM-05.1
30-14-2813(1)(b)	N/A	considering the nature of processing and the information available to the processor by assisting the controller in meeting the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a breach of security, as provided for in 30-14-1704, of the system of the processor to meet the controller's obligations; and	Functional	Intersects With	Data Privacy Requirements for Contractors & Service Providers	PRI-14	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		PRI-07.1
30-14-2813(1)(c)	N/A	providing necessary information to enable the controller to conduct and document data protection assessments.	Functional	Intersects With	Data Protection Impact Assessment (DPIA)	RSK-19	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.	5		RSK-10
30-14-2813(1)(c)	N/A	providing necessary information to enable the controller to conduct and document data protection assessments.	Functional	Intersects With	Data Privacy Requirements for Contractors & Service Providers	PRI-14	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		PRI-07.1
30-14-2813(2)	N/A	A contract between a controller and a processor must govern the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract must be binding and clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and obligations of both parties. The contract must also require that the processor:	Functional	Intersects With	Data Privacy Requirements for Contractors & Service Providers	PRI-14	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		PRI-07.1
30-14-2813(2)	N/A	A contract between a controller and a processor must govern the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract must be binding and clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and obligations of both parties. The contract must also require that the processor:	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	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		TPM-05
30-14-2813(2)	N/A	A contract between a controller and a processor must govern the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract must be binding and clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and obligations of both parties. The contract must also require that the processor:	Functional	Intersects With	Binding Corporate Rules (BCR)	PRI-15	Mechanisms exist to implement and manage Binding Corporate Rules (BCR) (e.g., data sharing agreement) to legally-bind all parties engaged in a joint economic activity that contractually states enforceable rights on data subjects with regard to the processing of their personal data.	5		PRI-01.5
30-14-2813(2)(a)	N/A	ensure that each person processing personal data is subject to a duty of confidentiality with respect to the personal data;	Functional	Intersects With	Confidentiality Agreements	HRS-07.1	Mechanisms exist to require Non-Disclosure Agreements (NDAs) or similar confidentiality agreements that reflect the needs to protect data and operational details, for both employees and third-parties.	8		HRS-06.1
30-14-2813(2)(a)	N/A	ensure that each person processing personal data is subject to a duty of confidentiality with respect to the personal data;	Functional	Intersects With	Security of Personal Data (PD)	PRI-10	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.	5		PRI-01.6

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **USA - Montana Consumer Data Privacy Act (CDPA) (2025)**
Focal Document URL: https://mca.legmt.gov/bills/mca/title_0300/chapter_0140/part_0280/sections_index.html
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-state-mt-cdpa-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	Legacy SCF #
30-14-2813(2)(b)	N/A	at the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law;	Functional	Intersects With	Personal Data (PD) Retention & Disposal	PRI-30	Mechanisms exist to: (1) Retain Personal Data (PD), including metadata, for an organization-defined time period to fulfill the purpose(s) identified in the notice or as required by law; (2) Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage; and (3) Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records).	8		PRI-05
30-14-2813(2)(b)	N/A	at the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law;	Functional	Intersects With	Cease Processing, Storing and/or Sharing Personal Data (PD)	PRI-29.2	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.	5		PRI-03.10
30-14-2813(2)(c)	N/A	on the reasonable request of the controller, make available to the controller all information in the processor's possession necessary to demonstrate the processor's compliance with the obligations in this part;	Functional	Intersects With	Ability To Demonstrate Conformity	CPL-04	Mechanisms exist to ensure the organization is able to demonstrate security, compliance and/or resilience capability conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.	8		CPL-01.3
30-14-2813(2)(c)	N/A	on the reasonable request of the controller, make available to the controller all information in the processor's possession necessary to demonstrate the processor's compliance with the obligations in this part;	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5		TPM-08
30-14-2813(2)(d)	N/A	engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the obligations of the processor with respect to the personal data; and	Functional	Subset Of	Contract Flow-Down Requirements	TPM-14.1	Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable subcontractors and suppliers.	10		TPM-05.2
30-14-2813(2)(d)	N/A	engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the obligations of the processor with respect to the personal data; and	Functional	Intersects With	Data Privacy Requirements for Contractors & Service Providers	PRI-14	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		PRI-07.1
30-14-2813(2)(e)	N/A	allow and cooperate with reasonable assessments by the controller or the controller's designated assessor, or the processor may arrange for a qualified and independent assessor to assess the processor's policies and technical and organizational measures in support of the obligations under this part using an appropriate and accepted control standard or framework and assessment procedure for the assessments. The processor shall provide a report of the assessment to the controller on request.	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	8		TPM-08
30-14-2813(2)(e)	N/A	allow and cooperate with reasonable assessments by the controller or the controller's designated assessor, or the processor may arrange for a qualified and independent assessor to assess the processor's policies and technical and organizational measures in support of the obligations under this part using an appropriate and accepted control standard or framework and assessment procedure for the assessments. The processor shall provide a report of the assessment to the controller on request.	Functional	Intersects With	Conformity Assessment	CPL-04.1	Mechanisms exist to conduct assessments to demonstrate security, compliance and/or resilience capability conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.	5		CPL-01.4
30-14-2813(2)(e)	N/A	allow and cooperate with reasonable assessments by the controller or the controller's designated assessor, or the processor may arrange for a qualified and independent assessor to assess the processor's policies and technical and organizational measures in support of the obligations under this part using an appropriate and accepted control standard or framework and assessment procedure for the assessments. The processor shall provide a report of the assessment to the controller on request.	Functional	Intersects With	Independent Assessors	CPL-08	Mechanisms exist to utilize independent assessors to evaluate security, compliance and resilience at planned intervals or when the Technology Asset, Application and/or Service (TAAS) undergoes significant changes.	5		CPL-03.1
30-14-2813(2)(e)	N/A	allow and cooperate with reasonable assessments by the controller or the controller's designated assessor, or the processor may arrange for a qualified and independent assessor to assess the processor's policies and technical and organizational measures in support of the obligations under this part using an appropriate and accepted control standard or framework and assessment procedure for the assessments. The processor shall provide a report of the assessment to the controller on request.	Functional	Intersects With	Third-Party Attestation (3PA)	TPM-23	Mechanisms exist to obtain an attestation from an independent Third-Party Assessment Organization (3PAO) that provides assurance of conformity with specified statutory, regulatory and contractual obligations for security, compliance and resilience controls, including any flow-down requirements to contractors and subcontractors.	5		TPM-05.8
30-14-2813(3)	N/A	Nothing in this section may be construed to relieve a controller or processor from the liabilities imposed on the controller or processor by virtue of the controller's or processor's role in the processing relationship, as described in this part.	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2813(4)	N/A	Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends on the following context in which personal data is to be processed:	Functional	Intersects With	Joint Processing of Personal Data (PD)	PRI-43	Mechanisms exist to clearly define and communicate the organization's role in processing Personal Data (PD) in the data processing ecosystem.	3		PRI-07.2
30-14-2813(4)(a)	N/A	A person who is not limited in the processing of personal data pursuant to a controller's instructions or who fails to adhere to a controller's instructions is a controller and not a processor with respect to a specific processing of data.	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2813(4)(b)	N/A	A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains a processor.	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2813(4)(c)	N/A	If a processor begins, alone or jointly with others, determining the purposes and means of the processing of personal data, the processor is a controller with respect to the processing and may be subject to an enforcement action under 30-14-2817.	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2814(1)	Data protection assessment	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. For the purposes of this section, processing that presents a heightened risk of harm to a consumer includes:	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-19	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		RSK-10
30-14-2814(1)	Data protection assessment	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. For the purposes of this section, processing that presents a heightened risk of harm to a consumer includes:	Functional	Intersects With	Instances Requiring A Risk Assessment	RSK-13.1	Mechanisms exist to define instances that require a risk assessment to be performed.	5		RSK-04.3
30-14-2814(1)(a)	N/A	the processing of personal data for the purposes of targeted advertising;	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-19	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		RSK-10
30-14-2814(1)(b)	N/A	the sale of personal data;	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-19	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		RSK-10
30-14-2814(1)(c)	N/A	the processing of personal data for the purposes of profiling in which the profiling presents a reasonably foreseeable risk of: (i) unfair or deceptive treatment of or unlawful disparate impact on consumers; (ii) financial, physical, or reputational injury to consumers; (iii) a physical or other form of intrusion on the solitude or seclusion or the private affairs or concerns of consumers in which the intrusion would be offensive to a reasonable person; or (iv) other substantial injury to consumers; and	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-19	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		RSK-10
30-14-2814(1)(d)	N/A	the processing of sensitive data.	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-19	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		RSK-10

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: USA - Montana Consumer Data Privacy Act (CDPA) (2025)
Focal Document URL: https://mca.legmt.gov/bills/mca/title_0300/chapter_0140/part_0280/sections_index.html
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-state-mt-cdpa-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	Legacy SCF #
30-14-2814(2)(a)	N/A	Data protection assessments conducted pursuant to subsection (1) must identify and weigh the benefits that may flow, directly and indirectly, 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 the processing as mitigated by safeguards that may be employed by the controller to reduce these risks.	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-19	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		RSK-10
30-14-2814(2)(b)	N/A	The controller shall factor into any data protection assessment the use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed.	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-19	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		RSK-10
30-14-2814(3)(a)	N/A	The attorney general may require that a controller disclose any data protection assessment that is relevant to an investigation conducted by the attorney general, and the controller shall make the data protection assessment available to the attorney general.	Functional	Intersects With	Data Protection Impact Assessment (DPIA)	RSK-19	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.	5		RSK-10
30-14-2814(3)(a)	N/A	The attorney general may require that a controller disclose any data protection assessment that is relevant to an investigation conducted by the attorney general, and the controller shall make the data protection assessment available to the attorney general.	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	CPL-27	Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required.	8		GOV-17
30-14-2814(3)(b)	N/A	The attorney general may evaluate the data protection assessment for compliance with the responsibilities set forth in this part.	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2814(3)(c)	N/A	Data protection assessments are confidential and are exempt from disclosure under the Freedom of Information Act, 5 U.S.C. 552.	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2814(3)(d)	N/A	To the extent any information contained in a data protection assessment disclosed to the attorney general includes information subject to attorney-client privilege or work product protection, the disclosure may not constitute a waiver of the privilege or protection.	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2814(4)	N/A	A single data protection assessment may address a comparable set of processing operations that include similar activities.	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-19	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		RSK-10
30-14-2814(5)	N/A	If a controller conducts a data protection assessment for the purpose of complying with another applicable law or regulation, the data protection assessment must be considered to satisfy the requirements established in this section if the data protection assessment is reasonably similar in scope and effect to the data protection assessment that would otherwise be conducted pursuant to this section.	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-19	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		RSK-10
30-14-2814(5)	N/A	If a controller conducts a data protection assessment for the purpose of complying with another applicable law or regulation, the data protection assessment must be considered to satisfy the requirements established in this section if the data protection assessment is reasonably similar in scope and effect to the data protection assessment that would otherwise be conducted pursuant to this section.	Functional	Intersects With	Control Reciprocity	CPL-14	Mechanisms exist to define instances of control reciprocity within assessment boundaries.	5		CPL-09
30-14-2814(6)	N/A	Data protection assessment requirements must apply to processing activities created or generated after January 1, 2025, and are not retroactive.	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2815(1)	De-identified data	Any controller in possession of de-identified data shall:	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2815(1)(a)	N/A	take reasonable measures to ensure that the de-identified data cannot be associated with an individual;	Functional	Intersects With	De-Identification (Anonymization)	DCH-36	Mechanisms exist to de-identify sensitive and/or regulated data through (1) Anonymization; (2) De-identification; (3) Pseudonymization; and/or (4) Redaction.	8		DCH-23
30-14-2815(1)(b)	N/A	publicly commit to maintaining and using de-identified data without attempting to re-identify the de-identified data; and	Functional	Subset Of	Data Privacy Notice	PRI-21	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		PRI-02
30-14-2815(1)(b)	N/A	publicly commit to maintaining and using de-identified data without attempting to re-identify the de-identified data; and	Functional	Intersects With	Dissemination of Data Privacy Program Information	PRI-20	Mechanisms exist to: (1) Ensure that the public has access to information about organizational data privacy activities and can communicate with its Chief Privacy Officer (CPO) or similar role; (2) Ensure that organizational data privacy practices are publicly available through organizational websites or document repositories; (3) Utilize publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to data privacy office(s) regarding data privacy practices; and (4) Inform data subjects when changes are made to the privacy notice and the nature of such changes.	5		PRI-01.3
30-14-2815(1)(c)	N/A	contractually obligate any recipients of the de-identified data to comply with all provisions of this part.	Functional	Subset Of	Data Privacy Requirements for Contractors & Service Providers	PRI-14	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.	10		PRI-07.1
30-14-2815(1)(c)	N/A	contractually obligate any recipients of the de-identified data to comply with all provisions of this part.	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	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).	5		TPM-05
30-14-2815(2)	N/A	Nothing in this part may be construed to: (a) require a controller or processor to re-identify de-identified data or pseudonymous data; or (b) maintain data in identifiable form or collect, obtain, retain, or access any data or technology to be capable of associating an authenticated consumer request with personal data.	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2815(3)	N/A	Nothing in this part may be construed to require a controller or processor to comply with an authenticated consumer rights request if the controller: (a) 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; (b) 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 (c) 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 in this section.	Functional	No Relationship	N/A	N/A	N/A	0		

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: USA - Montana Consumer Data Privacy Act (CDPA) (2025)
Focal Document URL: https://mca.legmt.gov/bills/mca/title_0300/chapter_0140/part_0280/sections_index.html
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-state-mt-cdpa-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	Legacy SCF #
30-14-2815(4)	N/A	The rights afforded under 30-14-2808(1)(a) through (1)(d) may not apply to pseudonymous data in cases in which the controller is able to demonstrate that 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	Intersects With	De-Identification (Anonymization)	DCH-36	Mechanisms exist to de-identify sensitive and/or regulated data through (1) Anonymization; (2) De-identification; (3) Pseudonymization; and/or (4) Redaction.	5		DCH-23
30-14-2815(4)	N/A	The rights afforded under 30-14-2808(1)(a) through (1)(d) may not apply to pseudonymous data in cases in which the controller is able to demonstrate that 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	Intersects With	Ability To Demonstrate Conformity	CPL-04	Mechanisms exist to ensure the organization is able to demonstrate security, compliance and/or resilience capability conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.	3		CPL-01.3
30-14-2815(5)	N/A	A controller that discloses pseudonymous data or de-identified data shall exercise reasonable oversight to monitor compliance with any contractual commitments to which the pseudonymous data or de-identified data is subject and shall take appropriate steps to address any breaches of those contractual commitments.	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	8		TPM-08
30-14-2815(5)	N/A	A controller that discloses pseudonymous data or de-identified data shall exercise reasonable oversight to monitor compliance with any contractual commitments to which the pseudonymous data or de-identified data is subject and shall take appropriate steps to address any breaches of those contractual commitments.	Functional	Intersects With	Data Privacy Requirements for Contractors & Service Providers	PRI-14	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		PRI-07.1
30-14-2815(5)	N/A	A controller that discloses pseudonymous data or de-identified data shall exercise reasonable oversight to monitor compliance with any contractual commitments to which the pseudonymous data or de-identified data is subject and shall take appropriate steps to address any breaches of those contractual commitments.	Functional	Intersects With	Third-Party Deficiency Remediation	TPM-18	Mechanisms exist to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.	5		TPM-09
30-14-2816(1)	Compliance by controller or processor	Nothing in this part may be construed to restrict a controller's or processor's ability to:	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2816(1)(a)	N/A	comply with federal, state, or municipal ordinances or regulations;	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2816(1)(b)	N/A	comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, municipal, or other government authorities;	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2816(1)(c)	N/A	cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state, or municipal ordinances or regulations;	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2816(1)(d)	N/A	investigate, establish, exercise, prepare for, or defend legal claims;	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2816(1)(e)	N/A	provide a product or service specifically requested by a consumer;	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2816(1)(f)	N/A	perform under a contract to which a consumer is a party, including fulfilling the terms of a written warranty;	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2816(1)(g)	N/A	take steps at the request of a consumer prior to entering a contract;	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2816(1)(h)	N/A	take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or another individual and when the processing cannot be manifestly based on another legal basis;	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2816(1)(i)	N/A	prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity, preserve the integrity or security of systems, or investigate, report, or prosecute those responsible for any of these actions;	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2816(1)(j)	N/A	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 that determines or similar independent oversight entities that determine: (i) whether the deletion of the information is likely to provide substantial benefits that do not exclusively accrue to the controller; (ii) the expected benefits of the research outweigh the privacy risks; and (iii) whether the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with re-identification;	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2816(1)(k)	N/A	assist another controller, processor, or third party with any of the obligations under this part; or	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2816(1)(l)	N/A	process personal data for reasons of public interest in public health, community health, or population health, but solely to the extent that the processing is: (i) subject to suitable and specific measures to safeguard the rights of the consumer whose personal data is being processed; and (ii) under the responsibility of a professional subject to confidentiality obligations under federal, state, or local law.	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2816(2)	N/A	The obligations imposed on controllers or processors under this part may not restrict a controller's or processor's ability to collect, use, or retain personal data for internal use to: (a) conduct internal research to develop, improve, or repair products, services, or technology; (b) effectuate a product recall; (c) identify and repair technical errors that impair existing or intended functionality; or (d) perform internal operations that are reasonably aligned with the expectations of the consumer or reasonably anticipated based on the consumer's existing relationship with the controller or 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	N/A	0		
30-14-2816(3)	N/A	The obligations imposed on controllers or processors under this part may not apply when compliance by the controller or processor with this part would violate an evidentiary privilege under the laws of this state. Nothing in this part may 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	N/A	0		
30-14-2816(4)	N/A	A controller or processor that discloses personal data to a processor or third-party controller in accordance with this part may not be considered to have violated this part if the processor or third-party controller that receives and processes the personal data violates this part provided, at the time the disclosing controller or processor disclosed the personal data, the disclosing controller or processor did not have actual knowledge that the receiving processor or third-party controller would violate this part. A receiving processor or third-party controller receiving personal data from a disclosing controller or processor in compliance with this part is likewise not in violation of this part for the transgressions of the disclosing controller or processor from which the receiving processor or third-party controller receives the personal data.	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2816(5)	N/A	Nothing in this part may be construed to: (a) impose any obligation on a controller or processor that adversely affects the rights or freedoms of any person, including but not limited to the rights of any person: (i) to freedom of speech or freedom of the press guaranteed in the first amendment to the United States constitution; or (ii) under Rule 504 of the Montana Rules of Evidence; (b) apply to a person's processing of personal data during the person's personal or household activities; or (c) require a controller or processor to implement an age verification or age-gating system or otherwise affirmatively collect the age of consumers, but a controller that chooses to conduct commercially reasonable age estimation to determine which consumers are minors is not liable for an erroneous age estimation.	Functional	No Relationship	N/A	N/A	N/A	0		

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: USA - Montana Consumer Data Privacy Act (CDPA) (2025)
Focal Document URL: https://mca.legmt.gov/bills/mca/title_0300/chapter_0140/part_0280/sections_index.html
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-state-mt-cdpa-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	Legacy SCF #
30-14-2816(6)	N/A	Personal data processed by a controller pursuant to this section may be processed to the extent that the processing is: (a) reasonably necessary and proportionate to the purposes listed in this section; and (b) adequate, relevant, and limited to what is necessary in relation to the specific purposes listed in this section. The controller or processor must, when applicable, consider the nature and purpose of the collection, use, or retention of the personal data collected, used, or retained pursuant to subsection (2). The personal data must be 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	Security of Personal Data (PD)	PRI-10	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		PRI-01.6
30-14-2816(6)	N/A	Personal data processed by a controller pursuant to this section may be processed to the extent that the processing is: (a) reasonably necessary and proportionate to the purposes listed in this section; and (b) adequate, relevant, and limited to what is necessary in relation to the specific purposes listed in this section. The controller or processor must, when applicable, consider the nature and purpose of the collection, use, or retention of the personal data collected, used, or retained pursuant to subsection (2). The personal data must be 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	Restrict Collection, Processing & Sharing To Identified Purpose	PRI-31.1	Mechanisms exist to minimize the collection, processing and/or sharing 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		PRI-04
30-14-2816(7)	N/A	If a controller processes personal data pursuant to an exemption in this section, the controller bears the burden of demonstrating that the processing qualifies for the exemption and complies with the requirements in subsection (6).	Functional	Intersects With	Ability To Demonstrate Conformity	CPL-04	Mechanisms exist to ensure the organization is able to demonstrate security, compliance and/or resilience capability conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.	8		CPL-01.3
30-14-2816(8)	N/A	Processing personal data for the purposes expressly identified in this section may not solely make a legal entity a controller with respect to the processing.	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2817(1)	Enforcement	The attorney general has exclusive authority and may use the duties and powers provided by Title 30, chapter 14, parts 1 and 2, to enforce violations pursuant to this part.	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2817(2)	N/A	The attorney general shall post on the attorney general's website: (a) information relating to: (i) the responsibilities of a controller pursuant to this part; (ii) the responsibilities of a processor pursuant to this part; and (iii) a consumer's rights pursuant to this part; and (b) an online mechanism through which a consumer may submit a complaint regarding consumer data privacy to the attorney general.	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2817(3)	N/A	(a) If the attorney general has reasonable cause to believe that a person has engaged in or is engaging in a violation of this part, the attorney general may issue a civil investigative demand pursuant to 30-14-113. (b) As part of a civil investigative demand, the attorney general may request 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 pursuant to this part.	Functional	Intersects With	Ability To Demonstrate Conformity	CPL-04	Mechanisms exist to ensure the organization is able to demonstrate security, compliance and/or resilience capability conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.	5		CPL-01.3
30-14-2817(3)	N/A	(a) If the attorney general has reasonable cause to believe that a person has engaged in or is engaging in a violation of this part, the attorney general may issue a civil investigative demand pursuant to 30-14-113. (b) As part of a civil investigative demand, the attorney general may request 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 pursuant to this part.	Functional	Intersects With	Data Protection Impact Assessment (DPIA)	RSK-19	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.	8		RSK-10
30-14-2817(4)	N/A	Actions brought by the department to enforce this part are subject to the statute of limitations pursuant to 27-2-231.	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2817(5)	N/A	Nothing in this part may be construed as providing the basis for or be subject to a private right of action for violations of this part or any other law.	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2818(1)	Responsibility according to role -- processing data of minors	A processor shall adhere to the instructions of a controller and shall assist the controller to meet the controller's obligations under 30-14-2811 and 30-14-2819, taking into account the nature of the processing and the information available to the processor. The processor shall assist the controller by:	Functional	Intersects With	Data Privacy Requirements for Contractors & Service Providers	PRI-14	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		PRI-07.1
30-14-2818(1)(a)	N/A	taking appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the controller's obligations under 30-14-2811; and	Functional	Intersects With	Data Privacy Requirements for Contractors & Service Providers	PRI-14	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		PRI-07.1
30-14-2818(1)(a)	N/A	taking appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the controller's obligations under 30-14-2811; and	Functional	Intersects With	Security of Personal Data (PD)	PRI-10	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.	5		PRI-01.6
30-14-2818(1)(b)	N/A	providing information to enable the controller to conduct and document data protection assessments pursuant to 30-14-2819.	Functional	Intersects With	Data Protection Impact Assessment (DPIA)	RSK-19	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.	5		RSK-10
30-14-2818(1)(b)	N/A	providing information to enable the controller to conduct and document data protection assessments pursuant to 30-14-2819.	Functional	Intersects With	Data Privacy Requirements for Contractors & Service Providers	PRI-14	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		PRI-07.1
30-14-2818(2)	N/A	A contract between a controller and a processor must satisfy the requirements of 30-14-2813(2).	Functional	Intersects With	Data Privacy Requirements for Contractors & Service Providers	PRI-14	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		PRI-07.1
30-14-2818(2)	N/A	A contract between a controller and a processor must satisfy the requirements of 30-14-2813(2).	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	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		TPM-05
30-14-2818(3)	N/A	Nothing in this section may be construed to relieve a controller or processor from the liabilities imposed on the controller or processor by virtue of the controller's or processor's role in the processing relationship as described in 30-14-2811 and 30-14-2819.	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2818(4)	N/A	Determining whether a person is acting as a controller or processor with respect to a specific processing of personal data is a fact-based determination that depends on the context in which personal data is to be processed. A person that is not limited in the person's processing of personal data pursuant to a controller's instructions or that fails to adhere to the instructions is a controller and not a processor with respect to a specific processing of personal data. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains a processor. If a processor begins, alone or jointly with others, determining the purposes and means of the processing of personal data, the processor is a controller with respect to the processing and may be subject to an enforcement action under 30-14-2817.	Functional	Intersects With	Joint Processing of Personal Data (PD)	PRI-43	Mechanisms exist to clearly define and communicate the organization's role in processing Personal Data (PD) in the data processing ecosystem.	3		PRI-07.2

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: USA - Montana Consumer Data Privacy Act (CDPA) (2025)
Focal Document URL: https://mca.legmt.gov/bills/mca/title_0300/chapter_0140/part_0280/sections_index.html
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-state-mt-cdpa-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	Legacy SCF #
30-14-2819(1)	Data protection assessments for heightened risk of harm to minors	A controller that, on or after October 1, 2025, offers an online service, product, or feature to a consumer whom the controller actually knows or willfully disregards is a minor shall conduct a data protection assessment for the online service, product, or feature if there is a heightened risk of harm to minors. The controller shall conduct the data protection assessment:	Functional	Intersects With	Data Protection Impact Assessment (DPIA)	RSK-19	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.	8		RSK-10
30-14-2819(1)	Data protection assessments for heightened risk of harm to minors	A controller that, on or after October 1, 2025, offers an online service, product, or feature to a consumer whom the controller actually knows or willfully disregards is a minor shall conduct a data protection assessment for the online service, product, or feature if there is a heightened risk of harm to minors. The controller shall conduct the data protection assessment:	Functional	Intersects With	Instances Requiring A Risk Assessment	RSK-13.1	Mechanisms exist to define instances that require a risk assessment to be performed.	5		RSK-04.3
30-14-2819(1)(a)	N/A	in a manner that is consistent with the requirements established in 30-14-2814; and	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-19	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		RSK-10
30-14-2819(1)(b)	N/A	to address: (i) the purpose of the online service, product, or feature; (ii) the categories of a minor's personal data that the online service, product, or feature processes; (iii) the purposes for which the controller processes a minor's personal data with respect to the online service, product, or feature; and (iv) a heightened risk of harm to minors that is a reasonably foreseeable result of offering the online service, product, or feature to minors.	Functional	Intersects With	Data Protection Impact Assessment (DPIA)	RSK-19	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.	8		RSK-10
30-14-2819(2)	N/A	A controller that conducts a data protection assessment pursuant to subsection (1) shall:	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2819(2)(a)	N/A	review the data protection assessment as necessary to account for a material change to the processing operations of the online service, product, or feature that is the subject of the data protection assessment; and	Functional	Intersects With	Data Protection Impact Assessment (DPIA)	RSK-19	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.	8		RSK-10
30-14-2819(2)(a)	N/A	review the data protection assessment as necessary to account for a material change to the processing operations of the online service, product, or feature that is the subject of the data protection assessment; and	Functional	Intersects With	Risk Assessment Update	RSK-13.2	Mechanisms exist to routinely update risk assessments and react accordingly upon identifying new security vulnerabilities, including using outside sources for security vulnerability information.	5		RSK-07
30-14-2819(2)(b)	N/A	maintain documentation concerning the data protection assessment for the longer of: (i) 3 years after the date on which the processing operations cease; or (ii) the date the controller ceases offering the online service, product, or feature.	Functional	Intersects With	Data Protection Impact Assessment (DPIA)	RSK-19	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.	5		RSK-10
30-14-2819(2)(b)	N/A	maintain documentation concerning the data protection assessment for the longer of: (i) 3 years after the date on which the processing operations cease; or (ii) the date the controller ceases offering the online service, product, or feature.	Functional	Intersects With	Media & Data Retention	DCH-27	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	5		DCH-18
30-14-2819(3)	N/A	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-19	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.	8		RSK-10
30-14-2819(4)	N/A	If a controller conducts a data protection assessment for the purpose of complying with another applicable law or regulation, the data protection assessment is considered to satisfy the requirements established in this section if the data protection assessment is reasonably similar in scope and effect to the data protection assessment that would otherwise be conducted pursuant to this section.	Functional	Intersects With	Data Protection Impact Assessment (DPIA)	RSK-19	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.	8		RSK-10
30-14-2819(4)	N/A	If a controller conducts a data protection assessment for the purpose of complying with another applicable law or regulation, the data protection assessment is considered to satisfy the requirements established in this section if the data protection assessment is reasonably similar in scope and effect to the data protection assessment that would otherwise be conducted pursuant to this section.	Functional	Intersects With	Control Reciprocity	CPL-14	Mechanisms exist to define instances of control reciprocity within assessment boundaries.	5		CPL-09
30-14-2819(5)	N/A	If a controller conducts a data protection assessment pursuant to subsection (1) or a data protection assessment review pursuant to subsection (2)(a) and determines that the online service, product, or feature that is the subject of the assessment poses a heightened risk of harm to minors, the controller shall establish and implement a plan to mitigate or eliminate the heightened risk.	Functional	Intersects With	Risk Response	RSK-16	Mechanisms exist to ensure proper risk response actions were performed to remediate findings from security, compliance and/or resilience-related: (1) Assessments; (2) Audits; and/or (3) Incidents.	5		RSK-06.1
30-14-2819(5)	N/A	If a controller conducts a data protection assessment pursuant to subsection (1) or a data protection assessment review pursuant to subsection (2)(a) and determines that the online service, product, or feature that is the subject of the assessment poses a heightened risk of harm to minors, the controller shall establish and implement a plan to mitigate or eliminate the heightened risk.	Functional	Intersects With	Risk Treatment Plan (RTP)	RSK-17.1	Mechanisms exist to formalize a Risk Treatment Plan (RTP) that applicable stakeholders will utilize to remediate identified risks according to a defined timeline.	8		RSK-06.4
30-14-2819(5)	N/A	If a controller conducts a data protection assessment pursuant to subsection (1) or a data protection assessment review pursuant to subsection (2)(a) and determines that the online service, product, or feature that is the subject of the assessment poses a heightened risk of harm to minors, the controller shall establish and implement a plan to mitigate or eliminate the heightened risk.	Functional	Intersects With	Data Protection Impact Assessment (DPIA)	RSK-19	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.	8		RSK-10
30-14-2819(6)	N/A	(a) A data protection assessment conducted pursuant to this section: (i) is confidential, except as provided in subsection (6)(b); and (ii) is not a public record and is exempt from public inspection and copying under the Freedom of Information Act, 5 U.S.C. 552. (b) (i) A controller shall make a data protection assessment conducted pursuant to this section available to the attorney general on request. The attorney general may evaluate the data protection assessment for compliance with this section and with other laws. (ii) The disclosure of a data protection assessment pursuant to a request from the attorney general does not constitute a waiver of any attorney-client privilege or work-product protection that might otherwise exist with respect to the assessment and any information in the assessment.	Functional	Intersects With	Data Protection Impact Assessment (DPIA)	RSK-19	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.	3		RSK-10
30-14-2819(6)	N/A	(a) A data protection assessment conducted pursuant to this section: (i) is confidential, except as provided in subsection (6)(b); and (ii) is not a public record and is exempt from public inspection and copying under the Freedom of Information Act, 5 U.S.C. 552. (b) (i) A controller shall make a data protection assessment conducted pursuant to this section available to the attorney general on request. The attorney general may evaluate the data protection assessment for compliance with this section and with other laws. (ii) The disclosure of a data protection assessment pursuant to a request from the attorney general does not constitute a waiver of any attorney-client privilege or work-product protection that might otherwise exist with respect to the assessment and any information in the assessment.	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	CPL-27	Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required.	5		GOV-17
30-14-2819(7)	N/A	Data protection assessment requirements apply to processing activities created or generated after October 1, 2025, and are not retroactive.	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2820(1)	Civil penalty injunction	A violation of this part is a violation of Title 30, chapter 14, parts 1 and 2.	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2820(2)	N/A	A person who violates the provisions of this part following the 30-day period described in 30-14-2817(3) is liable for a civil penalty in an amount not to exceed $7,500 for each violation.	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2820(3)	N/A	The attorney general may bring an action in the name of this state to: (a) recover a civil penalty under this section; (b) restrain or enjoin the person from violating this part; or (c) recover the civil penalty and seek injunctive relief.	Functional	No Relationship	N/A	N/A	N/A	0		
30-14-2820(4)	N/A	The attorney general may recover reasonable attorney fees and other reasonable expenses incurred in investigating and bringing an action under this section.	Functional	No Relationship	N/A	N/A	N/A	0		

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **USA - Montana Consumer Data Privacy Act (CDPA) (2025)**
Focal Document URL: https://mca.legmt.gov/bills/mca/title_0300/chapter_0140/part_0280/sections_index.html
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-state-mt-cdpa-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	Legacy SCF #
30-14-2820(5)	N/A	The attorney general shall deposit a civil penalty collected under this section in a special revenue account to the credit of the department pursuant to 30-14-143.	Functional	No Relationship	N/A	N/A	N/A	0		