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

**Reference Document :** Secure Controls Framework (SCF) version 2025.4
**STRM Guidance:** https://securecontrolsframework.com/set-theory-relationship-mapping-strm/

**Focal Document:** **OECD Privacy Principles**
**Focal Document URL:** https://oecdprivacy.org/
**Published STRM URL:** https://securecontrolsframework.com/content/strm/scf-strm-general-oecd-privacy-principles.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 |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Collection Limitation Principle | There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject. | Functional | Intersects With | Choice & Consent | PRI-03 | Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with:<br>(1) Plain language to illustrate the potential data privacy risks of the authorization;<br>(2) A means for users to decline the authorization; and<br>(3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations. | 8 | |
| 1 | Collection Limitation Principle | There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject. | Functional | Intersects With | Active Participation By Data Subjects | PRI-03.7 | Mechanisms exist to compel data subjects to select the level of consent deemed appropriate by the data subject for the relevant business purpose (e.g., opt-in, opt-out, accept all cookies, etc.). | 5 | |
| 1 | Collection Limitation Principle | There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject. | Functional | Intersects With | Authority To Collect, Process, Store & Share Personal Data (PD) | PRI-04.1 | Mechanisms exist to determine and document the legal authority that permits the organization to collect, receive, process, store, transmit, share, update and/or dispose Personal Data (PD), either generally or in support of a specific business process. | 5 | |
| 2 | Data Quality Principle | Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date. | Functional | Subset Of | Data Quality Management | PRI-10 | Mechanisms exist to manage the quality, utility, objectivity, integrity and impact determination and de-identification of sensitive/regulated data across the information lifecycle. | 10 | |
| 3 | Purpose Specification Principle | The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose. | Functional | Intersects With | Purpose Specification | PRI-02.1 | 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. | 8 | |
| 4 | Use Limitation Principle | Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except: | Functional | Intersects With | Continued Use of Personal Data (PD) | PRI-03.9 | Mechanisms exist to govern the continued use of Personal Data (PD) as it is collected, received, processed, stored, transmitted, shared and/or updated until:<br>(1) Disposal of PD occurs when there is no longer a legitimate business purpose;<br>(2) Disposal of PD occurs when the data retention timeline for the use case is met; and/or<br>(3) Continued use of PD is prohibited upon withdrawal of data subject consent. | 8 | |
| 4 | Use Limitation Principle | Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except: | Functional | Subset Of | Usage Restrictions of Personal Data (PD) | PRI-05.4 | Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:<br>(1) The purpose(s) originally collected, consistent with the data privacy notice(s);<br>(2) What is authorized by the data subject, or authorized agent; and<br>(3) What is consistent with applicable laws, regulations and contractual obligations. | 10 | |
| 4(a) | N/A | with the consent of the data subject; or | Functional | Intersects With | Choice & Consent | PRI-03 | Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with:<br>(1) Plain language to illustrate the potential data privacy risks of the authorization;<br>(2) A means for users to decline the authorization; and<br>(3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations. | 5 | |
| 4(b) | N/A | by the authority of law. | Functional | Intersects With | Authority To Collect, Process, Store & Share Personal Data (PD) | PRI-04.1 | Mechanisms exist to determine and document the legal authority that permits the organization to collect, receive, process, store, transmit, share, update and/or dispose Personal Data (PD), either generally or in support of a specific business process. | 5 | |
| 5 | Security Safeguards Principle | Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data. | Functional | Subset Of | Security of Personal Data (PD) | PRI-01.6 | Mechanisms exist to ensure Personal Data (PD) is protected by logical and physical security safeguards that are sufficient and appropriately scoped to protect the confidentiality and integrity of the PD. | 10 | |
| 6 | Openness Principle | There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller. | Functional | Subset Of | Dissemination of Data Privacy Program Information | PRI-01.3 | Mechanisms exist to:<br>(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;<br>(2) Ensure that organizational data privacy practices are publicly available through organizational websites or document repositories;<br>(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<br>(4) Inform data subjects when changes are made to the privacy notice and the nature of such changes. | 10 | |
| 7 | Individual Participation Principle | An individual should have the right: | Functional | no relationship | N/A | N/A | N/A | N/A | Nothing to map to |
| 7(a) | N/A | to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; | Functional | Intersects With | Data Subject Empowerment | PRI-06 | Mechanisms exist to provide authenticated data subjects the ability to:<br>(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;<br>(2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed;<br>(3) Obtain the source(s) of their PD;<br>(4) Obtain the categories of their PD being collected, received, processed, stored and shared;<br>(5) Request correction to their PD due to inaccuracies;<br>(6) Request erasure of their PD; and<br>(7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD. | 8 | |
| 7(b) | N/A | to have communicated to him, data relating to him | Functional | Intersects With | Personal Data (PD) Exports | PRI-06.7 | Mechanisms exist to export a data subject's available Personal Data (PD) in a readily usable format, upon an authenticated request. | 8 | |
| 7(b)(i) | N/A | within a reasonable time; | Functional | Intersects With | User Feedback Management | PRI-06.4 | Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes. | 8 | |
| 7(b)(ii) | N/A | at a charge, if any, that is not excessive; | Functional | Intersects With | User Feedback Management | PRI-06.4 | Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes. | 8 | |
| 7(b)(iii) | N/A | in a reasonable manner; and | Functional | Intersects With | User Feedback Management | PRI-06.4 | Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes. | 8 | |
| 7(b)(iv) | N/A | in a form that is readily intelligible to him; | Functional | Intersects With | Personal Data (PD) Exports | PRI-06.7 | Mechanisms exist to export a data subject's available Personal Data (PD) in a readily usable format, upon an authenticated request. | 8 | |
| 7(c) | N/A | to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and | Functional | Intersects With | User Feedback Management | PRI-06.4 | Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes. | 8 | |
| 7(d) | N/A | to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended. | Functional | Intersects With | User Feedback Management | PRI-06.4 | Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes. | 8 | |

| 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 |
|---|---|---|---|---|---|---|---|---|---|
| 8 | Accountability Principle | A data controller should be accountable for complying with measures which give effect to the principles stated above. | Functional | Subset Of | Data Privacy Program | PRI-01 | Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently. | 10 | |
| 8 | Accountability Principle | A data controller should be accountable for complying with measures which give effect to the principles stated above. | Functional | Intersects With | Chief Privacy Officer (CPO) | PRI-01.1 | Mechanisms exist to appoints a Chief Privacy Officer (CPO) or similar role, with the authority, mission, accountability and resources to coordinate, develop and implement, applicable data privacy requirements and manage data privacy risks through the organization-wide data privacy program. | 8 | |