

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

Reference Document: Secure Controls Framework (SCF) version 2026.2

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

Focal Document: **Switzerland - Federal Act on Data Protection (FADP) (2025)**

Focal Document URL: <https://www.admin.ch/opc/en/classified-compilation/19920153/index.html>

Published STRM URL: <https://content.securecontrolsframework.com/strm/scf-strm-emea-che-fadp-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
1	Purpose, Scope of Application and Federal Supervisory Authority	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
2	General Provisions	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
2.1	Definitions and Principles	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
2.1.5	Definitions	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
2.1.6	Principles	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
2.1.6.1	Principles	Personal data must be processed lawfully.	Functional	Intersects With	Reasonable Data Privacy Practices	PRI-01.11	Mechanisms exist to limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of Personal Data (PD) according to reasonable consumer expectations for what is necessary and proportionate.	5	
2.1.6.2	Principles	The processing must be carried out in good faith and be proportionate.	Functional	Intersects With	Reasonable Data Privacy Practices	PRI-01.11	Mechanisms exist to limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of Personal Data (PD) according to reasonable consumer expectations for what is necessary and proportionate.	5	
2.1.6.3	Principles	Personal data may only be collected for a specific purpose that the data subject can recognise; personal data may only be further processed in a manner that is compatible with this purpose.	Functional	Intersects With	Restrict Collection, Processing & Sharing To Identified Purpose	PRI-04	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	
2.1.6.4	Principles	They shall be destroyed or anonymised as soon as they are no longer required for the purpose of processing.	Functional	Intersects With	Personal Data (PD) Retention & Disposal	PRI-05	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	
2.1.6.5	Principles	Any person who processes personal data must satisfy themselves that the data are accurate. They must take all appropriate measures to correct, delete or destroy data that are incorrect or incomplete insofar as the purpose for which they are collected or processed is concerned. The appropriateness of the measures depends in particular on the form and the extent of the processing and on the risk that the processing poses to the data subject's personality or fundamental rights.	Functional	Intersects With	Personal Data (PD) Accuracy & Integrity	PRI-05.2	Mechanisms exist to ensure the accuracy and relevance of Personal Data (PD) throughout the information lifecycle by: (1) Keeping PD up-to-date; and (2) Remediating identified inaccuracies, as necessary.	5	
2.1.6.6	Principles	If the consent of the data subject is required, such consent is only valid if given voluntarily for one or more specific instances of processing based on appropriate information.	Functional	Intersects With	Data Subject Consent	PRI-03	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	
2.1.6.7	Principles	The consent must be explicitly given for:	Functional	Intersects With	Data Subject Consent	PRI-03	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	
2.1.6.7.a	Principles	processing sensitive personal data;	Functional	Intersects With	Data Subject Consent	PRI-03	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	
2.1.6.7.b	Principles	high-risk profiling by a private person; or	Functional	Intersects With	Data Subject Consent	PRI-03	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	
2.1.6.7.c	Principles	profiling by a federal body.	Functional	Intersects With	Data Subject Consent	PRI-03	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	
2.1.7	Data protection by design and data protection by default	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
2.1.7.1	Data protection by design and data protection by default	The controller is obliged to arrange the data processing in technical and organisational terms so that the data protection regulations, and in particular the principles under Article 6, are respected. It shall take account of this from the planning stage.	Functional	Intersects With	Reasonable Data Privacy Practices	PRI-01.11	Mechanisms exist to limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of Personal Data (PD) according to reasonable consumer expectations for what is necessary and proportionate.	5	
2.1.7.2	Data protection by design and data protection by default	The technical and organisational measures must in particular be appropriate with regard to the state of the art, the nature and the extent of the data processing and the risk that the processing poses to the data subject's personality or fundamental rights.	Functional	Intersects With	Security of Personal Data (PD)	PRI-01.6	Mechanisms exist to ensure Personal Data (PD) is protected by logical and physical security safeguards that are sufficient and appropriately scoped to protect the confidentiality and integrity of the PD.	5	
2.1.7.3	Data protection by design and data protection by default	The controller is obliged to ensure by means of suitable default settings that the processing of personal data is limited to the minimum required for the purpose intended, unless the data subject specifies otherwise.	Functional	Intersects With	Minimize Sensitive / Regulated Data	DCH-18.1	Mechanisms exist to minimize sensitive and/or regulated data that is collected, received, processed, stored and/or transmitted throughout the information lifecycle to only those elements necessary to support necessary business processes.	5	
2.1.7.3	Data protection by design and data protection by default	The controller is obliged to ensure by means of suitable default settings that the processing of personal data is limited to the minimum required for the purpose intended, unless the data subject specifies otherwise.	Functional	Intersects With	Collection Minimization	END-13.3	Mechanisms exist to utilize sensors that are configured to minimize the collection of information about individuals.	5	
2.1.8	Data security	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
2.1.8.1	Data security	The controller and the processor shall guarantee a level of data security appropriate to the risk by taking suitable technical and organisational measures.	Functional	Intersects With	Security of Personal Data (PD)	PRI-01.6	Mechanisms exist to ensure Personal Data (PD) is protected by logical and physical security safeguards that are sufficient and appropriately scoped to protect the confidentiality and integrity of the PD.	5	
2.1.8.2	Data security	The measures must make it possible to avoid breaches of data security.	Functional	Intersects With	Security of Personal Data (PD)	PRI-01.6	Mechanisms exist to ensure Personal Data (PD) is protected by logical and physical security safeguards that are sufficient and appropriately scoped to protect the confidentiality and integrity of the PD.	5	
2.1.8.3	Data security	The Federal Council shall issue provisions on the minimum requirements for data security.	Functional	No Relationship	N/A	N/A	N/A	0	
2.1.9	Processing by processors	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
2.1.9.1	Processing by processors	The processing of personal data may be assigned by contract or by the legislation to a processor it.	Functional	No Relationship	N/A	N/A	N/A	0	
2.1.9.1.a	Processing by processors	the data is processed only in the manner in which the controller itself is permitted to do it; and	Functional	No Relationship	N/A	N/A	N/A	0	

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
2.1.9.1.b	Processing by processors	no statutory or contractual duty of confidentiality prohibits assignment.	Functional	No Relationship	N/A	N/A	N/A	0	
2.1.9.2	Processing by processors	The controller must satisfy itself in particular that the processor is able to guarantee data security.	Functional	No Relationship	N/A	N/A	N/A	0	
2.1.9.3	Processing by processors	The processor may only assign processing to a third party with prior approval from the controller.	Functional	No Relationship	N/A	N/A	N/A	0	
2.1.9.4	Processing by processors	It may claim the same grounds for justification as the controller.	Functional	No Relationship	N/A	N/A	N/A	0	
2.1.10	Data protection officer	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
2.1.10.1	Data protection officer	Private controllers may appoint a data protection officer.	Functional	Intersects With	Data Protection Officer (DPO)	PRI-01.4	Mechanisms exist to appoint a Data Protection Officer (DPO): (1) Based on professional qualifications; and (2) To be involved in all issues related to how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed.	5	
2.1.10.2	Data protection officer	The data protection officer is the contact point for the data subjects and for the authorities responsible for data protection in Switzerland. He or she has the following tasks in particular:	Functional	Intersects With	Data Protection Officer (DPO)	PRI-01.4	Mechanisms exist to appoint a Data Protection Officer (DPO): (1) Based on professional qualifications; and (2) To be involved in all issues related to how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed.	5	
2.1.10.2.a	Data protection officer	training and advising the private controller in matters of data protection;	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5	
2.1.10.2.b	Data protection officer	providing support on applying the data protection regulations.	Functional	Intersects With	Data Protection Officer (DPO)	PRI-01.4	Mechanisms exist to appoint a Data Protection Officer (DPO): (1) Based on professional qualifications; and (2) To be involved in all issues related to how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed.	5	
2.1.10.3	Data protection officer	Private controllers may invoke the exception in Article 23 paragraph 4 if the following requirements are satisfied:	Functional	No Relationship	N/A	N/A	N/A	0	
2.1.10.3.a	Data protection officer	The data protection officer exercises his or her function towards the controller in a professionally independent manner and is not bound by any instructions.	Functional	No Relationship	N/A	N/A	N/A	0	
2.1.10.3.b	Data protection officer	He or she does not carry out any activities that are incompatible with his or her tasks as a data protection officer.	Functional	No Relationship	N/A	N/A	N/A	0	
2.1.10.3.c	Data protection officer	He or she has the required expertise.	Functional	No Relationship	N/A	N/A	N/A	0	
2.1.10.3.d	Data protection officer	The controller publishes the contact details of the data protection officer and notifies the FDPIC thereof.	Functional	No Relationship	N/A	N/A	N/A	0	
2.1.10.4	Data protection officer	The Federal Council shall regulate the appointment of data protection officers by federal bodies.	Functional	No Relationship	N/A	N/A	N/A	0	
2.1.11	Code of conduct	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
2.1.12	Record of processing activities	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
2.1.12.1	Record of processing activities	The controller and the processor shall each maintain a record of their processing activities.	Functional	Intersects With	Documenting Data Processing Activities	PRI-14	Mechanisms exist to document Personal Data (PD) processing activities that covers collection, receiving, processing, storage, transmission, sharing, updating and/or disposal actions with sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual requirements.	5	
2.1.12.2	Record of processing activities	The controller's record shall as a minimum contain:	Functional	Intersects With	Documenting Data Processing Activities	PRI-14	Mechanisms exist to document Personal Data (PD) processing activities that covers collection, receiving, processing, storage, transmission, sharing, updating and/or disposal actions with sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual requirements.	5	
2.1.12.2.a	Record of processing activities	the identity of the controller;	Functional	Intersects With	Documenting Data Processing Activities	PRI-14	Mechanisms exist to document Personal Data (PD) processing activities that covers collection, receiving, processing, storage, transmission, sharing, updating and/or disposal actions with sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual requirements.	5	
2.1.12.2.b	Record of processing activities	the purpose of processing;	Functional	Intersects With	Documenting Data Processing Activities	PRI-14	Mechanisms exist to document Personal Data (PD) processing activities that covers collection, receiving, processing, storage, transmission, sharing, updating and/or disposal actions with sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual requirements.	5	
2.1.12.2.c	Record of processing activities	a description of the categories of data subjects and the categories of processed personal data;	Functional	Intersects With	Documenting Data Processing Activities	PRI-14	Mechanisms exist to document Personal Data (PD) processing activities that covers collection, receiving, processing, storage, transmission, sharing, updating and/or disposal actions with sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual requirements.	5	
2.1.12.2.d	Record of processing activities	the categories of recipients;	Functional	Intersects With	Documenting Data Processing Activities	PRI-14	Mechanisms exist to document Personal Data (PD) processing activities that covers collection, receiving, processing, storage, transmission, sharing, updating and/or disposal actions with sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual requirements.	5	
2.1.12.2.e	Record of processing activities	if possible, the retention period for the personal data or the criteria for determining this period;	Functional	Intersects With	Documenting Data Processing Activities	PRI-14	Mechanisms exist to document Personal Data (PD) processing activities that covers collection, receiving, processing, storage, transmission, sharing, updating and/or disposal actions with sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual requirements.	5	
2.1.12.2.f	Record of processing activities	if possible, a general description of the measures taken to guarantee data security under Article 8;	Functional	Intersects With	Documenting Data Processing Activities	PRI-14	Mechanisms exist to document Personal Data (PD) processing activities that covers collection, receiving, processing, storage, transmission, sharing, updating and/or disposal actions with sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual requirements.	5	
2.1.12.2.g	Record of processing activities	if the data are disclosed abroad, details of the State concerned and the guarantees under Article 16 paragraph 2.	Functional	Intersects With	Documenting Data Processing Activities	PRI-14	Mechanisms exist to document Personal Data (PD) processing activities that covers collection, receiving, processing, storage, transmission, sharing, updating and/or disposal actions with sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual requirements.	5	
2.1.12.3	Record of processing activities	The processor's record shall contain information on identity of the processor and of the controller, the categories of processing carried out on behalf of the controller, and the information mentioned in paragraph 2 letters f and g.	Functional	Intersects With	Documenting Data Processing Activities	PRI-14	Mechanisms exist to document Personal Data (PD) processing activities that covers collection, receiving, processing, storage, transmission, sharing, updating and/or disposal actions with sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual requirements.	5	
2.1.12.4	Record of processing activities	The federal bodies shall notify the FDPIC of their records of processing activities.	Functional	No Relationship	N/A	N/A	N/A	0	
2.1.12.5	Record of processing activities	The Federal Council shall provide exceptions for legal entities that have fewer than 250 employees and whose data processing poses a negligible risk of harm to the personality of the data subjects.	Functional	No Relationship	N/A	N/A	N/A	0	
2.1.13	Certification	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
2.2	Data Processing by Private Controllers with Registered Office or Domicile Abroad	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
2.2.14	Representative	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
2.2.14.1	Representative	Private controllers with registered office or domicile abroad shall appoint a representative in Switzerland if they process the personal data of persons in Switzerland and the data processing meets the following requirements:	Functional	Intersects With	Localized Representation	CPL-08	Mechanisms exist to appoint localized representation with a physical presence in localities, as required by applicable laws and/or regulations.	5	
2.2.14.1.a	Representative	The processing is connected with the offer of goods or services or the monitoring of the behaviour of persons in Switzerland.	Functional	Intersects With	Compliance Scope	CPL-01.2	Mechanisms exist to document and validate the scope of security, compliance and resilience controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.	5	
2.2.14.1.b	Representative	The processing is on a large scale.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
2.2.14.1.c	Representative	The processing is carried out regularly.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
2.2.14.1.d	Representative	The processing poses a high risk to the personality of the data subjects.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
2.2.14.2	Representative	The representative shall serve as the contact point for the data subjects and the FDPIC.	Functional	Intersects With	Localized Representation	CPL-08	Mechanisms exist to appoint localized representation with a physical presence in localities, as required by applicable laws and/or regulations.	5	
2.2.14.3	Representative	The controller shall publish the name and the address of the representative.	Functional	Intersects With	Localized Representation	CPL-08	Mechanisms exist to appoint localized representation with a physical presence in localities, as required by applicable laws and/or regulations.	5	
2.2.15	Duties of the representative	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
2.2.15.1	Duties of the representative	The representative shall maintain a record of controller's processing activities that contains the information set out in Article 12 paragraph 2.	Functional	Intersects With	Documenting Data Processing Activities	PRI-14	Mechanisms exist to document Personal Data (PD) processing activities that covers collection, receiving, processing, storage, transmission, sharing, updating and/or disposal actions with sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual requirements.	5	
2.2.15.2	Duties of the representative	On request, he or she shall provide the FDPIC with the information contained in the record.	Functional	Intersects With	Investigation Access Restrictions	CPL-05.2	Mechanisms exist to support official investigations by provisioning government investigators with "least privileges" and "least functionality" to ensure that government investigators only have access to the Technology Assets, Applications, Services and/or Data (TAASD) needed to perform the investigation.	5	
2.2.15.3	Duties of the representative	On request, the representative shall provide data subjects with information on how they can exercise their rights.	Functional	Intersects With	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations; (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5	
2.3	Cross-Border Disclosure of Personal Data	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
2.3.16	Principles	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
2.3.16.1	Principles	Personal data may be disclosed abroad if the Federal Council has decided that the legislation of the State concerned or the international body guarantees an adequate level of protection.	Functional	Intersects With	Binding Corporate Rules (BCR)	PRI-01.5	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	
2.3.16.2	Principles	In the absence of a decision by the Federal Council under paragraph 1, personal data may be disclosed abroad only if an appropriate level of data protection is guaranteed by:	Functional	Intersects With	Binding Corporate Rules (BCR)	PRI-01.5	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	
2.3.16.2.a	Principles	a treaty under international law;	Functional	Intersects With	Binding Corporate Rules (BCR)	PRI-01.5	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	
2.3.16.2.b	Principles	data protection clauses in an agreement between the controller or the processor and its contractual partner, notice of which has been given to the FDPIC beforehand;	Functional	Intersects With	Binding Corporate Rules (BCR)	PRI-01.5	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	
2.3.16.2.c	Principles	specific guarantees drawn up by the competent federal body, notice of which has been given to the FDPIC beforehand;	Functional	Intersects With	Binding Corporate Rules (BCR)	PRI-01.5	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	
2.3.16.2.d	Principles	standard data protection clauses that the FDPIC has approved, issued or recognised beforehand; or	Functional	Intersects With	Binding Corporate Rules (BCR)	PRI-01.5	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	
2.3.16.2.e	Principles	binding corporate rules that have been approved in advance by the FDPIC or by the authority responsible for data protection in a State that guarantees an adequate level of protection.	Functional	Intersects With	Binding Corporate Rules (BCR)	PRI-01.5	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	
2.3.16.3	Principles	The Federal Council may provide for other appropriate guarantees in line with paragraph 2.	Functional	Intersects With	Binding Corporate Rules (BCR)	PRI-01.5	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	
2.3.17	Exceptions	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
2.3.18	Publication of personal data in electronic form	If personal data are made generally accessible by means of automated information and communications services in order to provide information to the general public, this is not deemed to be disclosure abroad, even if the data are accessible from abroad.	Functional	No Relationship	N/A	N/A	N/A	0	
3	Duties of the Controller and of the Processor	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
3.19	Duty to provide information when collecting personal data	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
3.19.1	Duty to provide information when collecting personal data	The controller shall inform the data subject in an appropriate manner when collecting personal data; this duty to provide information also applies if the data is not collected from the data subject.	Functional	Intersects With	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations; (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5	

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
3.19.2	Duty to provide information when collecting personal data	It shall provide the data subject on collecting the data with the information required for the data subject to exercise their rights under this Act and to guarantee transparent data processing; it shall provide the following information as a minimum:	Functional	Intersects With	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations; (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5	
3.19.2.a	Duty to provide information when collecting personal data	the controller's identity and contact details;	Functional	Intersects With	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations; (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5	
3.19.2.b	Duty to provide information when collecting personal data	the purpose of processing;	Functional	Intersects With	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations; (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5	
3.19.2.c	Duty to provide information when collecting personal data	if applicable, the recipients or the categories of recipients to which personal data is disclosed.	Functional	Intersects With	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations; (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5	
3.19.3	Duty to provide information when collecting personal data	If the data is not collected from the data subject, the controller shall also inform the data subject of the categories of processed personal data.	Functional	Intersects With	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/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	
3.19.4	Duty to provide information when collecting personal data	If the personal data are disclosed abroad, the controller shall also inform the data subject of the State or the international body to which such data are disclosed and if applicable of the guarantees under Article 16 paragraph 2 or the application of an exception under Article 17.	Functional	Intersects With	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations; (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5	
3.19.5	Duty to provide information when collecting personal data	If the data is not collected from the data subject, the controller shall also inform the data subject of the information specified in paragraphs 2–4 at the latest one month after receiving the data. If the controller discloses the personal data before the expiry of this deadline, it shall inform the data subject at the time of disclosure at the latest.	Functional	Intersects With	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations; (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5	
3.20	Exceptions from the duty to provide information and restrictions	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
3.21	Duty to provide information in the case of an automated individual decision	N/A	Functional	No Relationship	N/A	N/A	N/A	0	

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
3.21.1	Duty to provide information in the case of an automated individual decision	The controller shall inform the data subject about any decision that is based exclusively on automated processing and that has a legal consequence for or a considerable adverse effect on the data subject (automated individual decision).	Functional	Intersects With	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations; (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5	
3.21.2	Duty to provide information in the case of an automated individual decision	It shall on request allow the data subject to express their point of view. The data subject may request that the automated individual decision be reviewed by a natural person.	Functional	Intersects With	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/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	
3.21.3	Duty to provide information in the case of an automated individual decision	Paragraphs 1 and 2 do not apply if:	Functional	No Relationship	N/A	N/A	N/A	0	
3.21.3.a	Duty to provide information in the case of an automated individual decision	the automated individual decision is directly connected with the conclusion or the processing of a contract between the controller and the data subject and the data subject's request is granted; or	Functional	Intersects With	Automated Decision-Making Technology (ADMT) For Data Subject Actions	PRI-19	Mechanisms exist to ensure data subject actions utilizing Automated Decision-Making Technology (ADMT) where computation replaces, or substantially replaces, human decisionmaking, conforms with all applicable statutory, regulatory and/or contractual obligations.	5	
3.21.3.a	Duty to provide information in the case of an automated individual decision	the automated individual decision is directly connected with the conclusion or the processing of a contract between the controller and the data subject and the data subject's request is granted; or	Functional	Intersects With	Automated Decision-Making Technology (ADMT) Transparency	PRI-19.3	Mechanisms exist to provide data subjects with sufficient details of the logic and parameters used by Automated Decision-Making Technology (ADMT) to process the Personal Data (PD) to generate an output with respect to the data subject.	5	
3.21.3.b	Duty to provide information in the case of an automated individual decision	the data subject has explicitly consented to the decision being automated.	Functional	Intersects With	Automated Decision-Making Technology (ADMT) Opt-Out Consent	PRI-19.2	Mechanisms exist to provide concise, unambiguous and understandable instructions on how data subjects can opt-out of Automated Decision-Making Technology (ADMT).	5	
3.21.4	Duty to provide information in the case of an automated individual decision	If the automated individual decision is issued by a federal body, it must designate the decision accordingly. Paragraph 2 does not apply if, in accordance with Article 30 paragraph 2 of the Administrative Procedure Act of 20 December 1968 (APA) or another federal act, the data subject is not entitled to a hearing before the decision is taken.	Functional	No Relationship	N/A	N/A	N/A	0	
3.22	Data protection impact assessment	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
3.22.1	Data protection impact assessment	If processing is likely to result in a high risk to the data subject's personality or fundamental rights, the controller shall carry out a data protection impact assessment beforehand. If several similar processing procedures are planned, a joint assessment may be carried out.	Functional	Intersects With	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
3.22.2	Data protection impact assessment	The existence of a high risk, in particular when using new technologies, depends on the nature, extent, circumstances and purpose of the processing. A high risk arises in particular:	Functional	Intersects With	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
3.22.2.a	Data protection impact assessment	in the case of the large-scale processing of sensitive personal data;	Functional	Intersects With	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
3.22.2.b	Data protection impact assessment	if public areas are systematically monitored on a large scale.	Functional	Intersects With	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
3.22.3	Data protection impact assessment	The data protection impact assessment shall include a description of the planned processing, an evaluation of the risks to the data subject's personality or fundamental rights and a description of the measures to protect personality and fundamental rights.	Functional	Intersects With	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
3.22.4	Data protection impact assessment	Private controllers are exempt from having to carry out a data protection impact assessment if they are required by law to process the data.	Functional	Intersects With	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
3.22.5	Data protection impact assessment	A private controller may dispense with carrying out a data protection impact assessment if it uses a system, product or service that is certified under Article 13 for the intended use, or if it complies with a code of conduct under Article 11 that satisfies the following requirements:	Functional	Intersects With	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
3.22.5.a	Data protection impact assessment	The code of conduct is based on a data protection impact assessment.	Functional	Intersects With	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
3.22.5.b	Data protection impact assessment	It provides for measures to protect the personality and the data subject's fundamental rights.	Functional	Intersects With	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
3.22.5.c	Data protection impact assessment	It has been submitted to the FDPIC.	Functional	Intersects With	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
3.23	Consultation of the FDPIC	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
3.24	Notifications of data security breaches	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
3.24.1	Notifications of data security breaches	The controller shall notify the FDPIC of any breach of data security that is likely to lead to a high risk to the data subject's personality or fundamental rights as quickly as possible.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	
3.24.2	Notifications of data security breaches	In the notification, it shall as a minimum specify the nature of the breach of data security, its consequences and the measures taken or planned.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	
3.24.3	Notifications of data security breaches	The processor shall notify the controller of any breach of data security as quickly as possible.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	
3.24.4	Notifications of data security breaches	The controller shall inform the data subject if this is required for their protection or if the FDPIC so requests.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
3.24.5	Notifications of data security breaches	It may limit, delay or dispense with the provision of information to the data subject if:	Functional	Intersects With	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	
3.24.5.a	Notifications of data security breaches	there is a reason for doing so pursuant to Article 26 paragraph 1 letter b or paragraph 2 letter b or the provision of information is prohibited by a statutory duty of confidentiality;	Functional	Intersects With	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	
3.24.5.b	Notifications of data security breaches	the provision of information is impossible or requires disproportionate effort; or	Functional	Intersects With	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	
3.24.5.c	Notifications of data security breaches	the provision of information to the data subject is equally guaranteed by making a public announcement.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	
3.24.5bis	Notifications of data security breaches	With the controller's consent, the FDI/C may forward the notification to the National Cyber Security Centre for analysis. The communication may contain sensitive personal data, including data relating to administrative and criminal proceedings or sanctions involving the controller. 7	Functional	Intersects With	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	
3.24.6	Notifications of data security breaches	A notification made pursuant to this Article may only be used against the person required to notify in criminal proceedings with that person's consent.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	
4	Rights of the Data Subject	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
4.25	Right to information	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
4.25.1	Right to information	Any person may request information from the controller on whether personal data relating to them is being processed.	Functional	Intersects With	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/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	
4.25.2	Right to information	The data subject shall receive the information required to be able to exercise their rights under this Act and to guarantee transparent data processing. In every case, they are entitled to the following information:	Functional	Intersects With	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/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	
4.25.2.a	Right to information	the identity and the contact details of the controller;	Functional	Intersects With	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/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	
4.25.2.b	Right to information	the processed personal data as such;	Functional	Intersects With	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/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	
4.25.2.c	Right to information	the purpose of processing;	Functional	Intersects With	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/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	

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
4.25.2.d	Right to information	the retention period for the personal data or, if this is not possible, the criteria for determining this period;	Functional	Intersects With	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/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	
4.25.2.e	Right to information	the available information about the source of the personal data, if it has not been collected from the data subject;	Functional	Intersects With	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/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	
4.25.2.f	Right to information	if applicable, whether an automated individual decision has been taken and the logic behind the decision;	Functional	Intersects With	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/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	
4.25.2.g	Right to information	if applicable, the recipients or the categories of recipients to which personal data is disclosed, as well as the information specified in Article 19 paragraph 4.	Functional	Intersects With	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/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	
4.25.3	Right to information	The data subject may consent to having personal data relating to their health communicated by a health profession of their choice.	Functional	Intersects With	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/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	
4.25.4	Right to information	If the controller arranges for personal data to be processed by a processor, it remains under a duty to provide information.	Functional	Intersects With	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/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	
4.25.5	Right to information	No one may waive their right to information in advance.	Functional	Intersects With	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/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	
4.25.6	Right to information	The controller must provide information free of charge. The Federal Council may provide for exceptions, in particular if the effort required is disproportionate.	Functional	Intersects With	Reasonable Data Privacy Practices	PRI-01.11	Mechanisms exist to limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of Personal Data (PD) according to reasonable consumer expectations for what is necessary and proportionate.	5	
4.25.7	Right to information	The information shall in general be provided within 30 days.	Functional	Intersects With	Data Subject Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns and/or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
4.26	Limitations on the right to information	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
4.27	Limitation on the right to information for the media	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
4.28	Right to data portability	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
4.28.1	Right to data portability	Any person may request the controller to deliver the personal data that they have disclosed to it in a conventional electronic format if:	Functional	Intersects With	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/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	
4.28.1.a	Right to data portability	the controller is carrying out the automated processing of the data; and	Functional	Intersects With	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/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	
4.28.1.b	Right to data portability	the data are being processed with the consent of the data subject or in direct connection with the conclusion or the performance of a contract between the controller and the data subject.	Functional	Intersects With	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/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	
4.28.2	Right to data portability	The data subject may also request the controller to transfer their personal data to another controller if the requirements in paragraph 1 are met and no disproportionate effort is required.	Functional	Intersects With	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/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	
4.28.3	Right to data portability	The controller must deliver or transfer the personal data free of charge. The Federal Council may provide for exceptions, in particular if the effort is disproportionate.	Functional	Intersects With	Data Subject Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns and/or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	5	
4.29	Restrictions on the right to data portability	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
5	Special Provisions on Data Processing by Private Persons	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
5.30	Breaches of personality rights	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
5.30.1	Breaches of personality rights	Any person who processes personal data must not unlawfully breach the data subjects' personality rights.	Functional	Intersects With	Terms of Employment	HRS-05	Mechanisms exist to require all employees and contractors to apply cybersecurity and data protection principles in their daily work to <u>enable secure, compliant and resilient capabilities.</u>	5	
5.30.2	Breaches of personality rights	A breach of personality rights arises in particular if:	Functional	Intersects With	Terms of Employment	HRS-05	Mechanisms exist to require all employees and contractors to apply cybersecurity and data protection principles in their daily work to <u>enable secure, compliant and resilient capabilities.</u>	5	
5.30.2.a	Breaches of personality rights	personal data are processed contrary to the principles of Articles 6 and 8;	Functional	Intersects With	Terms of Employment	HRS-05	Mechanisms exist to require all employees and contractors to apply cybersecurity and data protection principles in their daily work to <u>enable secure, compliant and resilient capabilities.</u>	5	
5.30.2.b	Breaches of personality rights	personal data are processed contrary to the express wishes of the data subject;	Functional	Intersects With	Terms of Employment	HRS-05	Mechanisms exist to require all employees and contractors to apply cybersecurity and data protection principles in their daily work to <u>enable secure, compliant and resilient capabilities.</u>	5	
5.30.2.c	Breaches of personality rights	sensitive personal data are disclosed to third parties.	Functional	Intersects With	Terms of Employment	HRS-05	Mechanisms exist to require all employees and contractors to apply cybersecurity and data protection principles in their daily work to <u>enable secure, compliant and resilient capabilities.</u>	5	
5.30.3	Breaches of personality rights	In general no breach of personality rights arises if the data subject makes the personal data generally accessible and has not explicitly prohibited any processing.	Functional	Intersects With	Terms of Employment	HRS-05	Mechanisms exist to require all employees and contractors to apply cybersecurity and data protection principles in their daily work to <u>enable secure, compliant and resilient capabilities.</u>	5	
5.31	Grounds for justification	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
5.32	Legal rights	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
6	Special Provisions on Data Processing by Federal Bodies	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
6.33	Control and responsibility in the case of the joint processing of personal data	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
6.34	Legal basis	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
6.35	Automated data processing as part of pilot trials	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
6.36	Disclosure of personal data	N/A	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 2026.2

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

Focal Document: **Switzerland - Federal Act on Data Protection (FADP) (2025)**

Focal Document URL: <https://www.admin.ch/opc/en/classified-compilation/19920153/index.html>

Published STRM URL: <https://content.securecontrolsframework.com/strm/scf-strm-emea-che-fadp-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
6.36.1	Disclosure of personal data	Federal bodies may only disclose personal data if there is a statutory basis for doing so in accordance with Article 34 paragraphs 1–3.	Functional	No Relationship	N/A	N/A	N/A	0	
6.36.2	Disclosure of personal data	They may disclose personal data in specific cases in derogation from paragraph 1, if any one of the following requirements is satisfied:	Functional	No Relationship	N/A	N/A	N/A	0	
6.36.2.a	Disclosure of personal data	The data must be disclosed in order for the controller or the recipient to fulfil a statutory duty.	Functional	No Relationship	N/A	N/A	N/A	0	
6.36.2.b	Disclosure of personal data	The data subject has consented to disclosure.	Functional	No Relationship	N/A	N/A	N/A	0	
6.36.2.c	Disclosure of personal data	The data must be disclosed in order to protect the life or physical integrity of the data subject or of a third party and it is not possible to obtain the consent of the data subject within a reasonable time.	Functional	No Relationship	N/A	N/A	N/A	0	
6.36.2.d	Disclosure of personal data	The data subject has made their personal data generally accessible and has not explicitly prohibited any processing	Functional	No Relationship	N/A	N/A	N/A	0	
6.36.2.e	Disclosure of personal data	The recipient has credibly shown that the data subject has refused consent or objected to the disclosure in order to prevent the recipient from enforcing legal rights or exercising other legitimate interests; the data subject must be given the opportunity beforehand to comment, unless this is impossible or requires disproportionate effort.	Functional	No Relationship	N/A	N/A	N/A	0	
6.36.3	Disclosure of personal data	The federal bodies may furthermore disclose personal data as part of official information provided to the public or based on the Freedom of Information Act of 17 December 20049 if:	Functional	No Relationship	N/A	N/A	N/A	0	
6.36.3.a	Disclosure of personal data	the data is connected with the fulfilment of public duties; and	Functional	No Relationship	N/A	N/A	N/A	0	
6.36.3.b	Disclosure of personal data	there is an overriding public interest in the disclosure.	Functional	No Relationship	N/A	N/A	N/A	0	
6.36.4	Disclosure of personal data	They may also disclose a person's surname, first name, address and date of birth on request even if the requirements in paragraphs 1 or 2 are not satisfied.	Functional	No Relationship	N/A	N/A	N/A	0	
6.36.5	Disclosure of personal data	They may make personal data generally accessible by means of automated information and communications services if there is a legal basis for publishing the data or if they disclose data based on paragraph 3. If there is no longer a public interest in making the data generally accessible, the data concerned shall be deleted from the automated information and communications service.	Functional	No Relationship	N/A	N/A	N/A	0	
6.36.6	Disclosure of personal data	The federal bodies shall refuse or restrict disclosure or make disclosure subject to requirements if:	Functional	No Relationship	N/A	N/A	N/A	0	
6.36.6.a	Disclosure of personal data	essential public interests or the manifestly legitimate interests of the data subject so require; or	Functional	No Relationship	N/A	N/A	N/A	0	
6.36.6.b	Disclosure of personal data	statutory duties of confidentiality or special data protection regulations so require.	Functional	No Relationship	N/A	N/A	N/A	0	
6.37	Objecting to the disclosure of personal data	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
6.37.1	Objecting to the disclosure of personal data	A data subject who credibly shows a legitimate interest may object to the disclosure of specific personal data by the responsible federal body.	Functional	No Relationship	N/A	N/A	N/A	0	
6.37.2	Objecting to the disclosure of personal data	The federal body shall reject the objection if any one of the following requirements is satisfied:	Functional	No Relationship	N/A	N/A	N/A	0	
6.37.2.a	Objecting to the disclosure of personal data	There is a legal duty to disclose the data.	Functional	No Relationship	N/A	N/A	N/A	0	
6.37.2.b	Objecting to the disclosure of personal data	The fulfilment of the body's tasks would otherwise be jeopardised.	Functional	No Relationship	N/A	N/A	N/A	0	
6.37.3	Objecting to the disclosure of personal data	Article 36 paragraph 3 remains reserved.	Functional	No Relationship	N/A	N/A	N/A	0	
6.38	Offering documents to the Federal Archives	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
6.39	Data processing for purposes not related to specific persons	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
6.39.1	Data processing for purposes not related to specific persons	Federal bodies may process personal data for purposes not related to specific persons, in particular for research, planning or statistics, provided:	Functional	No Relationship	N/A	N/A	N/A	0	
6.39.1.a	Data processing for purposes not related to specific persons	the data are anonymised as soon as the purpose of processing permits;	Functional	No Relationship	N/A	N/A	N/A	0	
6.39.1.b	Data processing for purposes not related to specific persons	the federal body only discloses sensitive personal data to private persons in such a manner that the data subjects are not identifiable;	Functional	No Relationship	N/A	N/A	N/A	0	
6.39.1.c	Data processing for purposes not related to specific persons	the recipient only transmits the data to third parties with the consent of the federal body that disclosed the data; and	Functional	No Relationship	N/A	N/A	N/A	0	
6.39.1.d	Data processing for purposes not related to specific persons	the results are only published in such a manner that the data subjects are not identifiable.	Functional	No Relationship	N/A	N/A	N/A	0	
6.39.2	Data processing for purposes not related to specific persons	Articles 6 paragraph 3, 34 paragraph 2 and 36 paragraph 1 do not apply.	Functional	No Relationship	N/A	N/A	N/A	0	
6.40	Private law activities by federal bodies	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
6.41	Rights and procedures	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
6.41.1	Rights and procedures	Any person who has a legitimate interest may request the responsible federal body to:	Functional	No Relationship	N/A	N/A	N/A	0	
6.41.1.a	Rights and procedures	stop the unlawful processing of the personal data concerned;	Functional	No Relationship	N/A	N/A	N/A	0	
6.41.1.b	Rights and procedures	redress the consequences of unlawful processing;	Functional	No Relationship	N/A	N/A	N/A	0	
6.41.1.c	Rights and procedures	declare the processing to be unlawful.	Functional	No Relationship	N/A	N/A	N/A	0	
6.41.2	Rights and procedures	The applicant may in particular request the federal body to:	Functional	No Relationship	N/A	N/A	N/A	0	
6.41.2.a	Rights and procedures	correct, delete or destroy the personal data concerned;	Functional	No Relationship	N/A	N/A	N/A	0	
6.41.2.b	Rights and procedures	communicate its decision, in particular about correcting, deleting or destroying personal data, the objection against the disclosure under Article 37 or marking data as disputed under paragraph 4, to third parties or publish the decision.	Functional	No Relationship	N/A	N/A	N/A	0	
6.41.3	Rights and procedures	Instead of deleting or destroying the personal data, the federal body shall restrict the processing if:	Functional	No Relationship	N/A	N/A	N/A	0	
6.41.3.a	Rights and procedures	the data subject disputes the accuracy of the personal data and neither its accuracy nor its inaccuracy can be established;	Functional	No Relationship	N/A	N/A	N/A	0	
6.41.3.b	Rights and procedures	the overriding interests of third parties so require;	Functional	No Relationship	N/A	N/A	N/A	0	
6.41.3.c	Rights and procedures	an overriding public interest, in particular Switzerland's internal or external security, so requires;	Functional	No Relationship	N/A	N/A	N/A	0	
6.41.3.d	Rights and procedures	deleting or destroying the data may jeopardise an enquiry, an investigation or an administrative or judicial procedure.	Functional	No Relationship	N/A	N/A	N/A	0	
6.41.4	Rights and procedures	If neither the accuracy nor the inaccuracy of the relevant personal data can be established, the federal body shall mark the data as being disputed.	Functional	No Relationship	N/A	N/A	N/A	0	
6.41.5	Rights and procedures	The correction, deletion or destruction of personal data may not be requested in connection with the stocks held by publicly accessible libraries, education and training institutions, museums, archives or other public memory institutions. If the applicant credibly shows an overriding interest, he or she may request the institution to restrict access to the disputed data. Paragraphs 3 and 4 do not apply.	Functional	No Relationship	N/A	N/A	N/A	0	

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
6.41.6	Rights and procedures	The procedure is governed by the APA11. The exceptions in Articles 2 and 3 APA do not apply.	Functional	No Relationship	N/A	N/A	N/A	0	
6.42	Procedure for disclosing official documents that contain personal data	Where proceedings relating to access to official documents that contain personal data in accordance with the Freedom of Information Act of 17 December 2004 ¹² are pending, the data subject may claim those rights in the proceedings that they would have under Article 41 of this Act in relation to the documents that are the subject matter of the access proceedings.	Functional	No Relationship	N/A	N/A	N/A	0	
7	Federal Data Protection and Information Commissioner	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
7.1	Organisation	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
7.2	Investigation of Violations of Data Protection Regulations	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
7.2.49	Investigation	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
7.2.49.1	Investigation	The FDPIC shall open an investigation into a federal body or a private person ex officio or in response to a report if there are sufficient indications that a data processing activity could violate data protection regulations.	Functional	No Relationship	N/A	N/A	N/A	0	
7.2.49.2	Investigation	It may refrain from opening an investigation if the violation of data protection regulations is of minor importance.	Functional	No Relationship	N/A	N/A	N/A	0	
7.2.49.3	Investigation	The federal body or the private person shall provide the FDPIC with all the information and documents that is needed for the investigation. The right to refuse to provide information is governed by the Articles 16 and 17 of the APA ²⁰ , unless Article 50 paragraph 2 of this Act provides otherwise.	Functional	No Relationship	N/A	N/A	N/A	0	
7.2.49.4	Investigation	If the data subject has filed a report, the FDPIC shall inform them about the steps taken in response and the result of any investigation.	Functional	No Relationship	N/A	N/A	N/A	0	
7.2.50	Powers	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
7.2.51	Administrative measures	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
7.2.51.1	Administrative measures	If data protection regulations have been violated, the FDPIC may order that the processing be modified, suspended or terminated, wholly or in part, and the personal data deleted or destroyed, wholly or in part.	Functional	No Relationship	N/A	N/A	N/A	0	
7.2.51.2	Administrative measures	It may delay or prohibit disclosure abroad if this violates the requirements of Article 16 or 17 or provisions relating to the disclosure of personal data abroad in other federal acts.	Functional	No Relationship	N/A	N/A	N/A	0	
7.2.51.3	Administrative measures	It may in particular order that the federal body or the private person:	Functional	No Relationship	N/A	N/A	N/A	0	
7.2.51.3.a	Administrative measures	provide him or her with information in accordance with Articles 16 paragraph 2 letters b and c and 17 paragraph 2;	Functional	No Relationship	N/A	N/A	N/A	0	
7.2.51.3.b	Administrative measures	take the measures in accordance with Articles 7 and 8;	Functional	No Relationship	N/A	N/A	N/A	0	
7.2.51.3.c	Administrative measures	inform the data subjects in accordance with Articles 19 and 21;	Functional	No Relationship	N/A	N/A	N/A	0	
7.2.51.3.d	Administrative measures	conduct a data protection impact assessment in accordance with Article 22;	Functional	No Relationship	N/A	N/A	N/A	0	
7.2.51.3.e	Administrative measures	consult him or her in accordance with Article 23;	Functional	No Relationship	N/A	N/A	N/A	0	
7.2.51.3.f	Administrative measures	provide him or her or, if applicable, the data subject with information in accordance with Article 24;	Functional	No Relationship	N/A	N/A	N/A	0	
7.2.51.3.g	Administrative measures	provide the data subject with the information specified in Article 25.	Functional	No Relationship	N/A	N/A	N/A	0	
7.2.51.4	Administrative measures	It may also order that private controllers with registered office or domicile abroad appoint a representative in accordance with Article 14.	Functional	No Relationship	N/A	N/A	N/A	0	
7.2.51.5	Administrative measures	If the federal body or the private person has taken the required measures during the investigation in order to restore compliance with the data protection regulations, the FDPIC may simply issue an official warning.	Functional	No Relationship	N/A	N/A	N/A	0	
7.2.52	Procedure	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
7.2.53	Coordination	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
7.3	Administrative Assistance	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
7.3.54	Administrative assistance between Swiss authorities	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
7.3.55	Administrative assistance for foreign authorities	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
7.3.55.1	Administrative assistance for foreign authorities	The FDPIC may exchange information or personal data with foreign authorities that are responsible for data protection in order that they may fulfil their respective statutory duties in relation to data protection, provided the following requirements are satisfied:	Functional	No Relationship	N/A	N/A	N/A	0	
7.3.55.1.a	Administrative assistance for foreign authorities	Reciprocity with regard to administrative assistance is guaranteed.	Functional	No Relationship	N/A	N/A	N/A	0	
7.3.55.1.b	Administrative assistance for foreign authorities	The information and personal data are used only in the proceedings related to data protection that are the subject of the request for administrative assistance.	Functional	No Relationship	N/A	N/A	N/A	0	
7.3.55.1.c	Administrative assistance for foreign authorities	The recipient authority undertakes to preserve professional secrecy as well as trade and manufacturing secrecy.	Functional	No Relationship	N/A	N/A	N/A	0	
7.3.55.1.d	Administrative assistance for foreign authorities	The information and personal data are only disclosed to third parties if the authority that provided them gives its approval beforehand.	Functional	No Relationship	N/A	N/A	N/A	0	
7.3.55.1.e	Administrative assistance for foreign authorities	The recipient authority undertakes to comply with the requirements and restrictions imposed by the authority that provided the information and personal data.	Functional	No Relationship	N/A	N/A	N/A	0	
7.3.55.2	Administrative assistance for foreign authorities	In order to justify its request for administrative assistance or to comply with the request from an authority, the FDPIC may provide the following information in particular:	Functional	No Relationship	N/A	N/A	N/A	0	
7.3.55.2.a	Administrative assistance for foreign authorities	the identity of the controller, of the processor or of other third parties involved;	Functional	No Relationship	N/A	N/A	N/A	0	
7.3.55.2.b	Administrative assistance for foreign authorities	the categories of data subjects;	Functional	No Relationship	N/A	N/A	N/A	0	
7.3.55.2.c	Administrative assistance for foreign authorities	the identity the data subjects, provided:	Functional	No Relationship	N/A	N/A	N/A	0	
7.3.55.2.c.1	Administrative assistance for foreign authorities	the data subjects have consented, or	Functional	No Relationship	N/A	N/A	N/A	0	
7.3.55.2.c.2	Administrative assistance for foreign authorities	disclosure of the identity of the data subjects is essential for the FDPIC or the foreign authority to fulfil statutory duties;	Functional	No Relationship	N/A	N/A	N/A	0	
7.3.55.2.d	Administrative assistance for foreign authorities	processed personal data or categories of processed personal data;	Functional	No Relationship	N/A	N/A	N/A	0	
7.3.55.2.e	Administrative assistance for foreign authorities	the purpose of processing;	Functional	No Relationship	N/A	N/A	N/A	0	

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
7.3.55.2.f	Administrative assistance for foreign authorities	the recipients or the categories of recipients;	Functional	No Relationship	N/A	N/A	N/A	0	
7.3.55.2.g	Administrative assistance for foreign authorities	technical and organisational measures.	Functional	No Relationship	N/A	N/A	N/A	0	
7.3.55.3	Administrative assistance for foreign authorities	Before the FDPIC provides information that may include professional, trade or manufacturing secrets to a foreign authority, it shall inform the natural persons or legal entities concerned that hold these secrets, and invite them to comment, unless this is not possible or requires disproportionate effort.	Functional	No Relationship	N/A	N/A	N/A	0	
7.4	Other Tasks of the FDPIC	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
7.4.56	Register	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
7.4.57	Information	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
7.4.58	Further tasks	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
7.4.58.1	Further tasks	The FDPIC shall also carry out the following tasks in particular:	Functional	No Relationship	N/A	N/A	N/A	0	
7.4.58.1.a	Further tasks	It shall inform, train and advise federal bodies and private persons on data protection matters.	Functional	No Relationship	N/A	N/A	N/A	0	
7.4.58.1.b	Further tasks	It shall support the cantonal bodies and work with Swiss and foreign authorities that are responsible for data protection.	Functional	No Relationship	N/A	N/A	N/A	0	
7.4.58.1.c	Further tasks	It shall raise public awareness, and in particular that of persons in need of protection, in relation to data protection.	Functional	No Relationship	N/A	N/A	N/A	0	
7.4.58.1.d	Further tasks	It shall provide data subjects on request with information on how they may exercise their rights.	Functional	No Relationship	N/A	N/A	N/A	0	
7.4.58.1.e	Further tasks	It shall comment on draft federal legislation and measures that involve data processing.	Functional	No Relationship	N/A	N/A	N/A	0	
7.4.58.1.f	Further tasks	It shall carry out the duties assigned to it under the Freedom of Information Act of 17 December 2004 ²³ or other federal acts.	Functional	No Relationship	N/A	N/A	N/A	0	
7.4.58.1.g	Further tasks	It shall develop working instruments as recommendations of good practice for use by controllers, processors and data subjects; for this purpose, it shall take into account the specifics of the field concerned and the need to protect vulnerable persons.	Functional	No Relationship	N/A	N/A	N/A	0	
7.4.58.2	Further tasks	It may also advise federal bodies that are not subject to his or her supervision in accordance with Articles 2 and 4. The federal bodies may allow him or her to inspect files.	Functional	No Relationship	N/A	N/A	N/A	0	
7.4.58.3	Further tasks	The FDPIC has the power to declare to foreign authorities that are responsible for data protection that direct service is permitted in relation to data protection in Switzerland, provided Switzerland is granted reciprocal rights.	Functional	No Relationship	N/A	N/A	N/A	0	
7.5	Fees	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
8	Criminal Provisions	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
9	Conclusion of International Treaties	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
10	Final Provisions	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	