NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document : Secure Controls Framework (SCF) version 2025.3
STRM Guidance: https://securecontrolsframework.com/set-theory-relationship-mapping-strm/

Focal Document: Saudi Arabia Personal Data Protection Law (PDPL)
Focal Document URL: https://sdaia.gov.sa/en/SDAIA/about/Documents/Personal%20Data%20English%20V2-23April2023-%20Reviewed-.pdf
Published STRM URL: https://securecontrolsframework.com/content/strm/scf-strm-emea-sa-pdpl.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
Article 1	N/A	For the purpose of implementing this Law, the following terms shall have the meanings assigned thereto, unless the context requires otherwise: 1-Law: The Personal Data Protection Law. 2-Regulations: The Implementing Regulations of the Law. 3-Competent Authority: The authority to be determined by a resolution of the Council of Ministers. 4-Personal Data: Any data, regardless of its source or form, that may lead to identifying an individual specifically, or that may directly or indirectly make it possible to identify an individual, including name, personal identification number, addresses, contact numbers, license numbers, records, personal assets, bank and credit card numbers, photos and videos of an individual, and any other data of personal nature. 5-Processing: Any operation carried out on Personal Data by any means, whether manual or automated, including collecting, recording, saving, indexing, organizing, formatting, storing, modifying, updating, consolidating, retrieving, using, disclosing, transmitting, publishing, sharing, linking, blocking, erasing and destroying data. 6-Collection: The collection of Personal Data by Controller in accordance with the provisions of this Law, either from the Data Subject directly, a representative of the Data Subject, any legal guardian over the Data Subject or any other party. 7-Destruction: Any action taken on Personal Data that makes it unreadable and irretrievable, or impossible to identify the related Data Subject. 8-Disclosure: Enabling any person - other than the Controller or the Processor, as the case may be - to access, collect or use personal data by any means and for any purpose. 9-Transfer: The transfer of Personal Data from one place to another for Processing. 10-Publishing: Transmitting or making available any Personal Data using any written, audio or visual means.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 2.1	N/A	The Law applies to any Processing of Personal Data related to individuals that takes place in the Kingdom by any means, including the Processing of Personal Data related to individuals residing in the Kingdom by any means from any party outside the Kingdom. This includes the data of the deceased if it would lead to them or a member of their family being identified specifically.	Functional	subset of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
Article 2.2	N/A	The scope of applying the Law excludes the individual's Personal Data Processing for purposes that do not go beyond personal or family use, as long as the Data Subject did not publish or disclose it to others. The Regulations shall define personal and family use provided in this Paragraph.	Functional	intersects with	Compliance Scope	CPL-01.2	Mechanisms exist to document and validate the scope of cybersecurity and data protection controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.	8	
Article 3	N/A	The provisions and procedures stated in this Law shall not prejudice any provision that grants a right to the Data Subject or confers better protection to Personal Data pursuant to any other law or an international agreement to which the Kingdom is a party.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 4	N/A	Data Subject shall have the following rights pursuant to this Law and as set out in the Regulations:	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 4.1	N/A	The right to be informed about the legal basis and the purpose of the Collection of their Personal Data.	Functional	subset of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
Article 4.2	N/A	The right to access their Personal Data held by the Controller, in accordance with the rules and procedures set out in the Regulations, and without prejudice to the provisions of Article (9) of this Law.	Functional	intersects with	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	5	
Article 4.3	N/A	The right to request obtaining their Personal Data held by the Controller in a readable and clear format, in accordance with the controls and procedures specified by the Regulations.	Functional	intersects with	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	5	
Article 4.4	N/A	The right to request correcting, completing, or updating their Personal Data held by the Controller.	Functional	intersects with	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
Article 4.5	N/A	The right to request a Destruction of their Personal Data held by the Controller when such Personal Data is no longer needed by Data Subject, without prejudice to the provisions of Article (18) of this Law.	Functional	intersects with	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	5	
Article 5.1	N/A	Except for the cases stated in this Law, neither Personal Data may be processed nor the purpose of Personal Data Processing may be changed without the consent of the Data Subject. The Regulations Shall set out the conditions of the consent, the cases in which the consent must be explicit, and the terms and conditions related to obtaining the consent of the legal guardian if the Data Subject fully or partially lacks legal capacity.	Functional	intersects with	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, processing, storage, sharing, updating and disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; (2) A means for users to decline the authorization; and (3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	5	
Article 5.2	N/A	In all cases, Data Subject may withdraw the consent mentioned in Paragraph (1) of this Article at any time; the Regulations determines the necessary controls for such case.	Functional	intersects with	Revoke Consent	PRI-03.4	Mechanisms exist to allow data subjects to revoke consent to collect, receive, process, store, transmit, update and/or share their Personal Data (PD).	5	
Article 6	N/A	In the following cases, Processing of Personal Data shall not be subject to the consent referred to in Paragraph (1) of Article (5) herein:	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 6.1	N/A	If the Processing serves actual interests of the Data Subject, but communicating with the Data Subject is impossible or difficult.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 6.2	N/A	If the Processing is pursuant to another law or in implementation of a previous agreement to which the Data Subject is a party.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 6.3	N/A	If the Controller is a Public Entity and the Processing is required for security purposes or to satisfy judicial requirements.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 6.4	N/A	If the Processing is necessary for the purpose of legitimate interest of the Controller, without prejudice to the rights and interests of the Data Subject, and provided that no Sensitive Data is to be processed. Related provisions and controls are set out in the Regulations.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 7	N/A	The consent referred to in paragraph (1) of Article (5) of this Law may not form a condition of providing a service or a benefit, unless such service or benefit is directly related to the Processing of Personal Data for which the consent is given.	Functional	intersects with	Product or Service Delivery Restrictions	PRI-03.5	Mechanisms exist to prevent discrimination against a data subject for exercising their legal rights pertaining to modifying or revoking consent, including prohibiting: (1) Refusing products and/or services; (2) Charging different rates for goods and/or services; and (3) Providing different levels of quality.	5	
Article 8	N/A	Subject to the provisions of this Law and the Regulations regarding the Disclosure of Personal Data, the Controller shall only select Processors providing the necessary guarantees to implement the provisions of this Law and the Regulations. The Controller shall also monitor the compliance of said Processors with the provisions of this Law and the Regulations. This shall not prejudice the Controller's responsibilities towards the Data Subject or the Competent Authority as the case may be. The Regulations shall set out the provisions necessary in this regard, including provisions related to any subsequent contracts conducted by the Processor.	Functional	subset of	Information Sharing With Third Parties	PRI-07	Mechanisms exist to disclose Personal Data (PD) to third-parties only for the purposes identified in the data privacy notice and with the implicit or explicit consent of the data subject.	10	
Article 8	N/A	Subject to the provisions of this Law and the Regulations regarding the Disclosure of Personal Data, the Controller shall only select Processors providing the necessary guarantees to implement the provisions of this Law and the Regulations. The Controller shall also monitor the compliance of said Processors with the provisions of this Law and the Regulations. This shall not prejudice the Controller's responsibilities towards the Data Subject or the Competent Authority as the case may be. The Regulations shall set out the provisions necessary in this regard, including provisions related to any subsequent contracts conducted by the Processor.	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	
Article 8	N/A	Subject to the provisions of this Law and the Regulations regarding the Disclosure of Personal Data, the Controller shall only select Processors providing the necessary guarantees to implement the provisions of this Law and the Regulations. The Controller shall also monitor the compliance of said Processors with the provisions of this Law and the Regulations. This shall not prejudice the Controller's responsibilities towards the Data Subject or the Competent Authority as the case may be. The Regulations shall set out the provisions necessary in this regard, including provisions related to any subsequent contracts conducted by the Processor.	Functional	intersects with	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity and data protection controls.	5	
Article 9.1	N/A	The Controller may set time frames for exercising the right to access Personal Data stated in Paragraph (2) of Article (4) herein as stipulated in the Regulations. The Controller may limit the exercise of this right in the following cases:	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 9.1.a	N/A	If this is necessary to protect the Data Subject or other parties from any harm, according to the provisions set forth the Regulations.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 9.1.b	N/A	If the Controller is a Public Entity and the restriction is required for security purposes, required by another law, or required to fulfill judicial requirements.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 9.2	N/A	The Controller shall prevent the Data Subject from accessing Personal Data in any of the situations stated in Paragraphs (1, 2, 3, 4, 5) and (6) of Article (16) herein.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 10	N/A	The Controller may only collect Personal Data directly from the Data Subject and may only process Personal Data for the purposes for which they have been collected. However, the Controller may collect Personal Data from a source other that the Data Subject and may process Personal Data for purposes other than the ones for which they have been collected in the following situations: The Regulations shall set out the provisions, controls and procedures related to what is stated in paragraphs (2) to (7) of this Article.	Functional	intersects with	Primary Source Personal Data (PD) Collection	DCH-22.3	Mechanisms exist to collect Personal Data (PD) directly from the individual.	5	
Article 10	N/A	The Controller may only collect Personal Data directly from the Data Subject and may only process Personal Data for the purposes for which they have been collected. However, the Controller may collect Personal Data from a source other that the Data Subject and may process Personal Data for purposes other than the ones for which they have been collected in the following situations: The Regulations shall set out the provisions, controls and procedures related to what is stated in paragraphs (2) to (7) of this Article.	Functional	intersects with	Primary Sources	PRI-04.2	Mechanisms exist to ensure information is directly collected from the data subject, whenever possible.	5	
Article 10	N/A	The Controller may only collect Personal Data directly from the Data Subject and may only process Personal Data for the purposes for which they have been collected. However, the Controller may collect Personal Data from a source other that the Data Subject and may process Personal Data for purposes other than the ones for which they have been collected in the following situations: The Regulations shall set out the provisions, controls and procedures related to what is stated in paragraphs (2) to (7) of this Article.	Functional	subset of	Acquired Personal Data (PD)	PRI-04.4	Mechanisms exist to promptly inform data subjects of the utilization purpose when their Personal Data (PD) is acquired and not received directly from the data subject, except where that utilization purpose was disclosed in advance to the data subject.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
Article 10.1	N/A	The Data Subject gives their consent in accordance with the provisions of this Law.	Functional	intersects with	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, processing, storage, sharing, updating and disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; (2) A means for users to decline the authorization; and (3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	5	
Article 10.2	N/A	Personal Data is publicly available or was collected from a publicly available source.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 10.3	N/A	The Controller is a Public Entity, and the Collection or Processing of the Personal Data is required for public interest or security purposes, or to implement another law, or to fulfill judicial requirements.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 10.4	N/A	Complying with this may harm the Data Subject or affect their vital interests	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 10.5	N/A	Personal Data Collection or Processing is necessary to protect public health, public safety, or to protect the life or health of specific individuals.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 10.6	N/A	Personal Data is not to be recorded or stored in a form that makes it possible to directly or indirectly identify the Data Subject.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 10.7	N/A	Personal Data Collection is necessary to achieve legitimate interests of the Controller, without prejudice to the rights and interests of the Data Subject, and provided that no Sensitive Data is to be processed.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 11.1	N/A	The purpose for which Personal Data is collected shall be directly related to the Controller's purposes, and shall not contravene any legal provisions.	Functional	intersects with	Purpose Specification	PRI-02.1	Mechanisms exist to ensure the data privacy notice identifies the purpose(s) for which Personal Data (PD) is collected, received, processed, stored, transmitted, shared.	5	
Article 11.2	N/A	The methods and means of Personal Data Collection shall not conflict with any legal provisions, shall be appropriate for the circumstances of the Data Subject, shall be direct, clear and secure, and shall not involve any deception, misleading or extortion.	Functional	subset of	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	10	
Article 11.2	N/A	The methods and means of Personal Data Collection shall not conflict with any legal provisions, shall be appropriate for the circumstances of the Data Subject, shall be direct, clear and secure, and shall not involve any deception, misleading or extortion.	Functional	intersects with	Personal Data (PD) Collection Methods	PRI-04.7	Mechanisms exist to ensure that Personal Data (PD) collection methods are: (1) In accordance with applicable statutory and/or regulatory requirements; (2) Appropriate for the circumstances of the data subject; (3) Unambiguous; and (4) Secure.	5	
Article 11.3	N/A	The content of the Personal Data shall be appropriate and limited to the minimum amount necessary to achieve the purpose of the Collection. Content that may lead to specifically identifying Data Subject once the purpose of Collection is achieved shall be avoided. The Regulations shall set out the necessary controls in this regard.	Functional	intersects with	Minimize Sensitive / Regulated Data	DCH-18.1	Mechanisms exist to minimize sensitive/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	
Article 11.3	N/A	The content of the Personal Data shall be appropriate and limited to the minimum amount necessary to achieve the purpose of the Collection. Content that may lead to specifically identifying Data Subject once the purpose of Collection is achieved shall be avoided. The Regulations shall set out the necessary controls in this regard.	Functional	intersects with	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, updating and/or sharing Personal Data (PD) to: (1) The purpose(s) originally collected, consistent with the data privacy notice(s); (2) What is authorized by the data subject, or authorized agent; and (3) What is consistent with applicable laws, regulations and contractual obligations.	5	
Article 11.4	N/A	If the Personal Data collected is no longer necessary for the purpose for which it has been collected, the Controller shall, without undue delay, cease their Collection and destroy previously collected Personal Data.	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	
Article 12	N/A	The Controller shall use a privacy policy and make it available to Data Subjects for their information prior to collecting their Personal Data. The policy shall specify the purpose of Collection, Personal Data to be collected, the means used for Collection, Processing, storage and Destruction, and information about the Data Subject rights and how to exercise such rights.	Functional	equal	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
Article 13	N/A	When collecting Person Data directly from the Data Subject, the Controller shall take appropriate measures to inform the Data Subject of the following upon Collection:	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 13.1	N/A	The legal basis for collecting their Personal Data.	Functional	intersects with	Authority To Collect, Process, Store & Share Personal Data (PD)	PRI-04.1	Mechanisms exist to determine and document the legal authority that permits the organization to collect, receive, process, store, transmit, update and/or share Personal Data (PD), either generally or in support of a specific business process.	5	
Article 13.2	N/A	The purpose of the Collection, and shall specify the Personal Data whose Collection is mandatory and the Personal Data whose Collection is optional. The Data Subject shall be informed that the Personal Data will not be subsequently processed in a manner inconsistent with the Collection purpose or in cases other than those stated in Article (10) of this Law.	Functional	intersects with	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5	
Article 13.2	N/A	The purpose of the Collection, and shall specify the Personal Data whose Collection is mandatory and the Personal Data whose Collection is optional. The Data Subject shall be informed that the Personal Data will not be subsequently processed in a manner inconsistent with the Collection purpose or in cases other than those stated in Article (10) of this Law.	Functional	subset of	Purpose Specification	PRI-02.1	Mechanisms exist to ensure the data privacy notice identifies the purpose(s) for which Personal Data (PD) is collected, received, processed, stored, transmitted, shared.	10	
Article 13.3	N/A	Unless the Collection is for security purposes, the identity of the person collecting the Personal Data and the address of its representative, if necessary.	Functional	intersects with	Purpose Specification	PRI-02.1	Mechanisms exist to ensure the data privacy notice identifies the purpose(s) for which Personal Data (PD) is collected, received, processed, stored, transmitted, shared.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
Article 13.4	N/A	The entities to which the Personal Data will be disclosed, the capacity of such entities, and whether the Personal Data will be transferred, disclosed or processed outside the Kingdom.	Functional	subset of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
Article 13.5	N/A	The potential consequences and risks that may result from not collecting the Personal Data.	Functional	subset of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
Article 13.6	N/A	The rights of the Data Subject pursuant to Article (4) herein.	Functional	subset of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
Article 13.7	N/A	Such other elements as set out in the Regulations based on the nature of the activity done by the Controller.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 14	N/A	The Controller may not process Personal Data without taking sufficient steps to verify the Personal Data accuracy, completeness, timeliness and relevance to the purpose for which it is collected in accordance with the provisions of the Law.	Functional	intersects with	Acquired Personal Data (PD)	PRI-04.4	Mechanisms exist to promptly inform data subjects of the utilization purpose when their Personal Data (PD) is acquired and not received directly from the data subject, except where that utilization purpose was disclosed in advance to the data subject.	5	
Article 14	N/A	The Controller may not process Personal Data without taking sufficient steps to verify the Personal Data accuracy, completeness, timeliness and relevance to the purpose for which it is collected in accordance with the provisions of the Law.	Functional	intersects with	Validate Collected Personal Data (PD)	PRI-04.5	Mechanisms exist to ensure that the data subject, or authorized representative, validate Personal Data (PD) during the collection process.	5	
Article 14	N/A	The Controller may not process Personal Data without taking sufficient steps to verify the Personal Data accuracy, completeness, timeliness and relevance to the purpose for which it is collected in accordance with the provisions of the Law.	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	
Article 15	N/A	The Controller may not Disclose Personal Data except in the following situations: The Regulations shall set out the provisions, controls and procedures related to what is stated in paragraphs (2) to (6) of this Article.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 15.1	N/A	Data Subject consents to the Disclosure in accordance with the provisions of the Law.	Functional	intersects with	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, processing, storage, sharing, updating and disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; (2) A means for users to decline the authorization; and (3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	5	
Article 15.2	N/A	Personal Data has been collected from a publicly available source.	Functional	intersects with	Acquired Personal Data (PD)	PRI-04.4	Mechanisms exist to promptly inform data subjects of the utilization purpose when their Personal Data (PD) is acquired and not received directly from the data subject, except where that utilization purpose was disclosed in advance to the data subject.	5	
Article 15.3	N/A	The entity requesting Disclosure is a Public Entity, and the Collection or Processing of the Personal Data is required for public interest or security purposes, or to implement another law, to fulfill judicial requirements.	Functional	intersects with	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive / regulated data to authorized parties with a need to know.	5	
Article 15.4	N/A	The Disclosure is necessary to protect public health, public safety, or to protect the lives or health of specific individuals.	Functional	intersects with	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive / regulated data to authorized parties with a need to know.	5	
Article 15.5	N/A	The Disclosure will only involve subsequent Processing in a form that makes it impossible to directly or indirectly identify the Data Subject.	Functional	intersects with	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive / regulated data to authorized parties with a need to know.	5	
Article 15.6	N/A	The Disclosure is necessary to achieve legitimate interests of the Controller, without prejudice to the rights and interests of the Data Subject, and provided that no Sensitive Data is to be processed.	Functional	intersects with	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive / regulated data to authorized parties with a need to know.	5	
Article 16	N/A	The Controller shall not disclose Personal Data in the situations stated in Paragraphs (1, 2, 5) and (6) of Article (15) if the Disclosure:	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 16.1	N/A	Represents a threat to security, harms the reputation of the Kingdom, or conflicts with the interests of the Kingdom.	Functional	intersects with	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive / regulated data to authorized parties with a need to know.	5	
Article 16.2	N/A	Affects the Kingdom's relations with any other state.	Functional	intersects with	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive / regulated data to authorized parties with a need to know.	5	
Article 16.3	N/A	Prevents the detection of a crime, affects the rights of an accused to a fair trial, or affects the integrity of existing criminal procedures.	Functional	intersects with	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive / regulated data to authorized parties with a need to know.	5	
Article 16.4	N/A	Compromises the safety of an individual.	Functional	intersects with	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive / regulated data to authorized parties with a need to know.	5	
Article 16.5	N/A	Results in violating the privacy of an individual other than the Data Subject, as set out in the Regulations.	Functional	intersects with	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive / regulated data to authorized parties with a need to know.	5	
Article 16.6	N/A	Conflicts with the interests of a person that fully or partially lacks legal capacity.	Functional	intersects with	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive / regulated data to authorized parties with a need to know.	5	
Article 16.7	N/A	Violates legally established professional obligations.	Functional	intersects with	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive / regulated data to authorized parties with a need to know.	5	
Article 16.8	N/A	Involves a violation of an obligation, procedure, or judicial decision.	Functional	intersects with	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive / regulated data to authorized parties with a need to know.	5	
Article 16.9	N/A	Exposes the identity of a confidential source of information in a manner detrimental to the public interest.	Functional	intersects with	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive / regulated data to authorized parties with a need to know.	5	
Article 17.1	N/A	If Personal Data is corrected, completed or updated, the Controller shall notify such amendment to all the other entities to which such Personal Data has been transferred and make the amendment available to such entities.	Functional	intersects with	Updating & Correcting Personal Data (PD)	DCH-22.1	Mechanisms exist to utilize technical controls to correct Personal Data (PD) that is inaccurate or outdated, incorrectly determined regarding impact, or incorrectly de-identified.	5	
Article 17.1	N/A	If Personal Data is corrected, completed or updated, the Controller shall notify such amendment to all the other entities to which such Personal Data has been transferred and make the amendment available to such entities.	Functional	intersects with	Updating Personal Data (PD)	PRI-12	Mechanisms exist to develop processes to identify and record the method under which Personal Data (PD) is updated and the frequency that such updates occur.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
Article 17.2	N/A	The Regulations shall set out the time frames for correction and updating of Personal Data, types of correction, and the procedures required to avoid the consequences of Processing incorrect, inaccurate or outdated Personal Data.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 18.1	N/A	The Controller shall, without undue delay, Destroy the Personal Data when no longer necessary for the purpose for which they were collected. However, the Controller may retain data after the purpose of the Collection ceases to exist; provided that it does not contain anything that may lead to specifically identifying Data Subject pursuant to the controls stipulated in the Regulations.	Functional	subset of	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).	10	
Article 18.2	N/A	In the following cases, the Controller shall retain the Personal Data after the purpose of the Collection ceases to exist:	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 18.2.a	N/A	If there is a legal basis for retaining the Personal Data for a specific period, in which case the Personal Data shall be destroyed upon the lapse of that period or when the purpose of the Collection is satisfied, whichever longer.	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	
Article 18.2.b	N/A	If the Personal Data is closely related to a case under consideration before a judicial authority and the retention of the Personal Data is required for that purpose, in which case the Personal Data shall be destroyed once the judicial procedures are concluded.	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	
Article 19	N/A	The Controller shall implement all the necessary organizational, administrative and technical measures to protect Personal Data, including during the Transfer of Personal Data, in accordance with the provisions and controls set out in the Regulations.	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	
Article 20.1	N/A	The Controller shall notify the Competent Authority upon knowing of any breach, damage, or illegal access to personal data, in accordance with the Regulations.	Functional	intersects with	Data Breach	IRO-04.1	Mechanisms exist to address data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations.	5	
Article 20.2	N/A	The Controller shall notify the Data Subject of any breach, damage or illegal access to their Personal Data that would cause damage to their data or cause prejudice to their rights and interests, in accordance with the Regulations.	Functional	intersects with	Data Breach	IRO-04.1	Mechanisms exist to address data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations.	5	
Article 21	N/A	The Controller shall respond to the requests of the Data Subject pertaining to their rights under this Law within such period and in such method as set out in the Regulations.	Functional	subset of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	10	
Article 22	N/A	The Controller shall conduct an impact assessment of Personal Data Processing in relation to any product or service, based on the nature of the activity carried out by the Controller, in accordance with the relevant provisions of the Regulations.	Functional	equal	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	
Article 23	N/A	Without prejudice to this Law, the Regulations shall set out additional controls and procedures for the Processing of Health Data in a manner that ensures the privacy of the Data Subject and protects their rights under this Law. Such additional controls and procedures shall include the following:	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 23.1	N/A	Restricting the right to access Health Data, including medical files, to the minimum number of employees or workers and only to the extent necessary to provide the required Health Services.	Functional	intersects with	Limiting Personal Data (PD) Disclosures	PRI-01.7	Mechanisms exist to limit the disclosure of Personal Data (PD) to authorized parties for the sole purpose for which the PD was obtained.	5	
Article 23.2	N/A	Restricting Health Data Processing procedures and operations to the minimum extent possible of employees and workers as necessary to provide Health Services or offer health insurance programs.	Functional	intersects with	Limiting Personal Data (PD) Disclosures	PRI-01.7	Mechanisms exist to limit the disclosure of Personal Data (PD) to authorized parties for the sole purpose for which the PD was obtained.	5	
Article 24	N/A	Without prejudice to this Law, the Regulations shall set out additional controls and procedures for the Processing of Credit Data in a manner that ensures the privacy of the Data Subject and protects their rights under this Law and the Credit Information Law. Such controls and procedures shall include the following:	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 24.1	N/A	Implementing appropriate measures to verify that the Data Subject has given their explicit consent to the Collection of the Personal Data, changing the purpose of the Collection, or Disclosure or Publishing of the Personal Data in accordance with the provisions of this Law and the Credit Information Law.	Functional	intersects with	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, processing, storage, sharing, updating and disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; (2) A means for users to decline the authorization; and (3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	5	
Article 24.2	N/A	Requiring that the Data Subject be notified when a request for Disclosure of their Credit Data is received from any entity.	Functional	intersects with	Notification of Disclosure Request To Data Subject	PRI-14.2	Mechanisms exist to notify data subjects of applicable legal requests to disclose Personal Data (PD).	5	
Article 25	N/A	With the exception of the awareness-raising materials sent by Public Entities, Controller may not use personal means of communication, including the post and email, of the Data Subject to send advertising or awareness-raising materials, unless:	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 25.1	N/A	Obtaining the prior consent of the targeted recipient for such materials.	Functional	intersects with	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, processing, storage, sharing, updating and disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; (2) A means for users to decline the authorization; and (3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	5	
Article 25.2	N/A	The sender of the material shall provide a clear mechanism, as set out in the Regulations, that enables the targeted recipient to request stopping receiving such materials if they desire so.	Functional	intersects with	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, processing, storage, sharing, updating and disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; (2) A means for users to decline the authorization; and (3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
Article 25.3	N/A	The Regulations shall set out the provisions concerning the aforementioned advertising and awareness-raising materials, as well as the conditions and situations concerning the consent of the recipient to receive aforementioned materials.	Functional	intersects with	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, processing, storage, sharing, updating and disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; (2) A means for users to decline the authorization; and (3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	5	
Article 26	N/A	With the exception of Sensitive Data, Personal Data may be processed for marketing purposes, if it is collected directly from the Data Subject and their consent is given in accordance with the provisions of Law; the Regulations shall set out the controls in such regard.	Functional	intersects with	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, processing, storage, sharing, updating and disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; (2) A means for users to decline the authorization; and (3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	5	
Article 27	N/A	Personal data may be collected or processed for scientific, research, or statistical purposes without the consent of the Data Subject in the following situations:	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 27.1	N/A	If it does not specifically identify the Data Subject.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 27.2	N/A	If evidence of the Data Subject's identity will be destroyed during the Processing and prior to Disclosure of such data to any other entity, if it is not Sensitive Data.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 27.3	N/A	If personal data is collected or processed for these purposes is required by another law or in implementation of a previous agreement to which the Data Subject is a party. The Regulations shall set out the controls required by the provisions of this Article.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 28	N/A	It is not permissible to copy official documents where Data Subjects are identifiable, except where it is required by law, or when a competent public authority requests copying such documents pursuant to the Regulations.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 29.1	N/A	Subject to the provisions of Paragraph (2) of this Article, a Controller may Transfer Personal Data outside the Kingdom or disclose it to a party outside the Kingdom, in order to achieve any of the following purposes:	Functional	subset of	Transfer of Sensitive and/or Regulated Data	DCH-25	Mechanisms exist to restrict and govern the transfer of sensitive and/or regulated data to third-countries or international organizations.	10	
Article 29.1.a	N/A	If this is relating to performing an obligation under an agreement, to which the Kingdom is a party.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 29.1.b	N/A	If it is to serve the interests of the Kingdom.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 29.1.c	N/A	If this is to the performance of an obligation to which the Data Subject is a party	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 29.1.d	N/A	If this is to fulfill other purposes as set out in the Regulations.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 29.2	N/A	The conditions that must be met when there is a Transfer or Disclosure of Personal Data, according to what is stated in Paragraph (1) of this Article, are as follows:	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 29.2.a	N/A	The Transfer or Disclosure shall not cause any prejudice to national security or the vital interests of the Kingdom.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 29.2.a	N/A	The Transfer or Disclosure shall not cause any prejudice to national security or the vital interests of the Kingdom.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 29.2.b	N/A	There is an adequate level of protection for Personal Data outside the Kingdom. Such level of protection shall be at least equivalent to the level of protection guaranteed by the Law and Regulations, according to the results of an assessment conducted by the Competent Authority in coordination with whomever it deems appropriate from the other relevant authorities.	Functional	subset of	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.	10	
Article 29.2.c	N/A	The Transfer or Disclosure shall be limited to the minimum amount of Personal Data needed.	Functional	intersects with	Limiting Personal Data (PD) Disclosures	PRI-01.7	Mechanisms exist to limit the disclosure of Personal Data (PD) to authorized parties for the sole purpose for which the PD was obtained.	5	
Article 29.3	N/A	Paragraph (2) of this Article shall not apply to cases of extreme necessity to preserve the life or vital interests of the Data Subject or to prevent, examine or treat disease.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 29.4	N/A	The Regulations shall set out the provisions, criteria and procedures related to the implementing this Article, including applicable exceptions for Controllers regarding conditions referred to in Subparagraphs (b) and (c) of Paragraph (2) of this Article, as well as controls and procedures for such exemptions.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 30.1	N/A	Without prejudice to the provisions of this Law and the powers of the Saudi Central Bank pursuant to applicable legal provisions, the Competent Authority shall be the entity in charge of overseeing the implementation of this Law and the Regulations.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 30.2	N/A	The Regulations shall identify the situations where the Controller shall appoint one or more persons as personal data protection officer(s). and shall set the responsibilities of any such person in accordance with the provisions of this Law.	Functional	subset of	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10	
Article 30.2	N/A	The Regulations shall identify the situations where the Controller shall appoint one or more persons as personal data protection officer(s). and shall set the responsibilities of any such person in accordance with the provisions of this Law.	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 and disposed.	5	
Article 30.3	N/A	The Controller shall cooperate with the Competent Authority in performing its duties to supervise the implementation of the provisions of this Law and the Regulations, and shall take such steps as necessary in connection with the related matters referred to the Controller by the Competent Authority.	Functional	subset of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
Article 30.4	N/A	The Competent Authority, in order to carry out its duties related to supervising the implementation of the provisions of the Law and Regulations, may:	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 30.4.a	N/A	Request the necessary documents or information from the Controller to ensure its compliance with the provisions of the Law and Regulations.	Functional	subset of	Ability To Demonstrate Conformity	CPL-01.3	Mechanisms exist to ensure the organization is able to demonstrate conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.	10	
Article 30.4.b	N/A	Request the cooperation of any other party for the purposes of support in accomplishing supervisory duties and enforcement of the provisions of the Law and Regulations.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 30.4.c	N/A	Specify the appropriate tools and mechanisms for monitoring Controllers' compliance with the provisions of the Law and the Regulations, including maintaining a national register of Controllers for this purpose.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 30.4.d	N/A	Provide services related to Personal Data protection through the national register referred to in Subparagraph (c) of this Paragraph or through any other means deemed appropriate. The Competent Authority may collect a fee for the Personal Data protection services it may provide.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 30.5	N/A	The Competent Authority may, at its discretion, delegate to other authorities the accomplishment of some of its duties that are related to supervision or enforcement of the provisions of the Law and Regulations.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 31	N/A	Without prejudice to Article (18) herein, the Controller shall maintain records, for such a period as required under the Regulations, of the Personal Data Processing activities, based on the nature of the activity carried out by the Controller. Such records are to be available whenever requested by the Competent Authority. The records shall contain the following information at a minimum:	Functional	subset of	Documenting Data Processing Activities	PRI-14	Mechanisms exist to document Personal Data (PD) processing activities that cover collecting, receiving, processing, storing, transmitting, updating, sharing and disposal actions with sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual requirements.	10	
Article 31.1	N/A	Contact details of the Controller.	Functional	subset of	Documenting Data Processing Activities	PRI-14	Mechanisms exist to document Personal Data (PD) processing activities that cover collecting, receiving, processing, storing, transmitting, updating, sharing and disposal actions with sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual requirements.	10	
Article 31.2	N/A	The purpose of the Personal Data Processing.	Functional	subset of	Documenting Data Processing Activities	PRI-14	Mechanisms exist to document Personal Data (PD) processing activities that cover collecting, receiving, processing, storing, transmitting, updating, sharing and disposal actions with sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual requirements.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
Article 31.3	N/A	Description of the categories of Personal Data Subjects.	Functional	subset of	Documenting Data Processing Activities	PRI-14	Mechanisms exist to document Personal Data (PD) processing activities that cover collecting, receiving, processing, storing, transmitting, updating, sharing and disposal actions with sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual requirements.	10	
Article 31.4	N/A	Any other entity to which Personal Data has been, or will be, disclosed.	Functional	subset of	Documenting Data Processing Activities	PRI-14	Mechanisms exist to document Personal Data (PD) processing activities that cover collecting, receiving, processing, storing, transmitting, updating, sharing and disposal actions with sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual requirements.	10	
Article 31.5	N/A	Whether the Personal Data has been or will be transferred outside the Kingdom or disclosed to an entity outside the Kingdom.	Functional	subset of	Documenting Data Processing Activities	PRI-14	Mechanisms exist to document Personal Data (PD) processing activities that cover collecting, receiving, processing, storing, transmitting, updating, sharing and disposal actions with sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual requirements.	10	
Article 31.6	N/A	The expected period for which Personal Data shall be retained.	Functional	subset of	Documenting Data Processing Activities	PRI-14	Mechanisms exist to document Personal Data (PD) processing activities that cover collecting, receiving, processing, storing, transmitting, updating, sharing and disposal actions with sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual requirements.	10	
Article 31.6	N/A	The expected period for which Personal Data shall be retained.	Functional	subset of	Documenting Data Processing Activities	PRI-14	Mechanisms exist to document Personal Data (PD) processing activities that cover collecting, receiving, processing, storing, transmitting, updating, sharing and disposal actions with sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual requirements.	10	
Article 32	N/A	Repealed.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 33.1	N/A	The Competent Authority shall set the requirements for practicing commercial, professional or non-profit activities related to Personal Data protection in the Kingdom, in coordination with the competent authorities, and without prejudice to the other requirements set by those authorities in their domain of competence.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 33.2	N/A	The Competent Authority may grant licenses to entities that issue accreditation certificates to Controllers and Processors. The Competent Authority shall set the rules to regulate the issuance of such certificates.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 33.3	N/A	The Competent Authority may grant licenses to entities that conduct audits or checks of Personal Data Processing activities related to the Controller's activity, in accordance with the provisions stipulated in the Regulations. The Competent Authority shall set the conditions and criteria to grant such licenses, and the rules regulating them.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 33.4	N/A	The Competent Authority shall specify the appropriate tools and mechanisms to monitor compliance of Controllers and Processors outside the Kingdom in regard with their obligations as stated in the Law and the Regulations when Processing personal data related to individuals residing in the Kingdom by any means, and shall define procedures to enforce the provisions of the Law and the Regulations outside the Kingdom.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 34	N/A	A Data Subject may submit to the Competent Authority any complaint that may arise out of the implementation of this Law and the Regulations. The Regulations shall set out the rules for processing the complaints that may arise from implementing this Law and the Regulations.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 35.1	N/A	Without prejudice to any harsher penalty stipulated in another law, any individual discloses or publishes Sensitive Data, in violation of the provisions of the Law, with the intention of harming the Data Subject or achieving a personal benefit shall be punished with imprisonment for a period not exceeding (two years), or a fine not exceeding (three million) Riyals, or both.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 35.2	N/A	The Public Prosecution is responsible for investigating and prosecuting before the competent court for the violation stipulated in Paragraph (1) of this Article.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 35.3	N/A	The competent court shall be in charge of lawsuits arising from the implementation of this Article and issuing the prescribed penalties.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 35.4	N/A	The competent court may double the fine penalty stipulated in Paragraph (1) of this Article in the case of recidivism, even if it results in exceeding its maximum limit, provided that it does not exceed double this limit.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 36.1	N/A	In cases that are not covered in Article (35) herein and without prejudice to any harsher penalty stipulated in another law, a warning or a fine not exceeding (five million) Riyals shall be imposed on every person with a special natural or legal capacity - covered by the provisions of the Law - who violates any of the provisions of the Law or the Regulations. The fine penalty may be doubled in the event of a repeat violation, even if it results in exceeding its maximum limit, provided that it does not exceed double this limit.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 36.2	N/A	A committee (or more) shall be formed by a decision of the president of the Competent Authority. The number of its members shall not be less than (three), and one of them shall be appointed as the committee head, and there shall be a technical specialist and a legal advisor among them. The committee is to examine violations and issue warnings or impose fines as stipulated in Paragraph (1) of this Article, considering the type of violation committed, its seriousness and the extent of its impact; provided that the decision of the committee is approved by the president of the Competent Authority or whomever they delegate. The president of the Competent Authority shall issue, by their decision, the rules of work of the committee, and the remunerations of its members shall be determined therein.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 36.3	N/A	Anyone against whom a decision has been issued by the committee mentioned in Paragraph (2) of this Article has the right to appeal against them before the competent court.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 37.1	N/A	Employees and workers appointed by a decision of the president of the Competent Authority shall have the powers to control and inspect the violations stated in this Law or the Regulations. The president of the Competent Authority shall issue the rules and procedures in regard to the work of those employees and workers in accordance with the applicable laws.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 37.2	N/A	The employees and workers referred to in Paragraph (1) of this Article may seek assistance from criminal investigations authorities or other competent authorities to carry out their duties concerning control and inspection of violations stipulated in the Law or Regulations.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 37.3	N/A	The Competent Authority has the right to seize the means or tools used in committing the violation until a decision is made on it.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 38.1	N/A	Without prejudice to the rights of bona fide third parties, the competent court may order the confiscation of funds obtained as a result of committing the violations stipulated in the Law.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 38.2	N/A	The competent court, or the committee referred to in paragraph (2) of Article (36), as the case may be, may include in their penalty judgment or decision a provision that a summary of such judgment or decision shall be published at the expense of the violator in one (or more) local newspapers distributed in their area of residence, or using any other proper means. This is based on the type, seriousness and impact of the violation; provided that the publishing shall be after the judgment becomes final, the lapse of the deadline for appeals, or the issuance of a final ruling dismissing the appeal against the judgement.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 39	N/A	Without prejudice to the provisions of Article (35) and Paragraph (1) of Article (36) of this Law, the Public Entity shall discipline any of its employees who violate any of the provisions of this Law and Regulations, in accordance with the disciplinary provisions and procedures prescribed by law.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 40	N/A	Without prejudice to the penalties stated in this Law, any individual that suffers a damage as a result of any of the violations stated in this Law or the Regulations may apply to a competent court for proportionate compensation for the material or moral damage.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
Article 41	N/A	Any person that engages in the Processing of Personal Data shall protect the confidentiality of the Personal Data even after the end of such person's occupational or contractual relationship.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 42	N/A	The president of the Competent Authority shall issue the Regulations within a period not exceeding (seven hundred and twenty) days commencing on the date of publishing the Law provided that the president must coordinate before issuing the Law with: (Ministry of Communications and Information Technology, Ministry of Foreign Affairs, Communications, Space & Technology Commission, Digital Government Authority, National Cybersecurity Authority, Saudi Health Council, and Saudi Central Bank), each in its own jurisdiction.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
Article 43	N/A	This Law shall come into force after (seven hundred and twenty) days commencing on the date of its publication in the Official Gazette.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.