NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document : Secure Controls Framework (SCF) version 2025.1
STRM Guidance: https://securecontrolsframework.com/set-theory-relationship-mapping-strm/

Focal Document: **Regulation (EU) 2016/679 - General Data Protection Regulation (GDPR)**
Focal Document URL: https://commission.europa.eu/law/law-topic/data-protection/legal-framework-eu-data-protection_en
Published STRM URL: https://securecontrolsframework.com/content/strm/scf-strm-emea-eu-gdpr.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	Subject-matter and objectives	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 1.1	N/A	This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 1.2	N/A	This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 1.3	N/A	The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 2	Material scope	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 2.1	N/A	This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 2.2	N/A	This Regulation does not apply to the processing of personal data:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 2.2(a)	N/A	in the course of an activity which falls outside the scope of Union law;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 2.2(b)	N/A	by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 2.2(c)	N/A	by a natural person in the course of a purely personal or household activity;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 2.2(d)	N/A	by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 2.3	N/A	For the processing of personal data by the Union institutions, bodies, offices and agencies, Regulation (EC) No 45/2001 applies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data shall be adapted to the principles and rules of this Regulation in accordance with Article 98.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 2.4	N/A	This Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 3	Territorial scope	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 3.1	N/A	This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.	Functional	intersects with	Compliance Scope	CPL-01.2	Mechanisms exist to document and validate the scope of cybersecurity & data privacy controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.	5	
Article 3.2	N/A	This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:	Functional	intersects with	Compliance Scope	CPL-01.2	Mechanisms exist to document and validate the scope of cybersecurity & data privacy controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.	5	
Article 3.2(a)	N/A	the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or	Functional	intersects with	Compliance Scope	CPL-01.2	Mechanisms exist to document and validate the scope of cybersecurity & data privacy controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.	5	
Article 3.2(b)	N/A	the monitoring of their behaviour as far as their behaviour takes place within the Union.	Functional	intersects with	Compliance Scope	CPL-01.2	Mechanisms exist to document and validate the scope of cybersecurity & data privacy controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.	5	
Article 3.3	N/A	This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.	Functional	intersects with	Compliance Scope	CPL-01.2	Mechanisms exist to document and validate the scope of cybersecurity & data privacy controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.	5	
Article 4	Definitions	See source document for specific definitions	Functional	subset of	Standardized Terminology	SEA-02.1	Mechanisms exist to standardize technology and process terminology to reduce confusion amongst groups and departments.	10	
Article 5	Principles relating to processing of personal data	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 5.1	N/A	Personal data shall be:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 5.1(a)	N/A	processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');	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 5.1(b)	N/A	collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');	Functional	intersects with	Restrict Collection To Identified Purpose	PRI-04	Mechanisms exist to minimize the collection of Personal Data (PD) to only what is adequate, relevant and limited to the purposes identified in the data privacy notice, including protections against collecting PD from minors without appropriate parental or legal guardian consent.	5	
Article 5.1(c)	N/A	adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');	Functional	intersects with	Restrict Collection To Identified Purpose	PRI-04	Mechanisms exist to minimize the collection of Personal Data (PD) to only what is adequate, relevant and limited to the purposes identified in the data privacy notice, including protections against collecting PD from minors without appropriate parental or legal guardian consent.	5	
Article 5.1(d)	N/A	accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');	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 5.1(e)	N/A	kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');	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 5.1(e)	N/A	kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');	Functional	intersects with	Personal Data (PD) Formats	PRI-05.8	Mechanisms exist to retain Personal Data (PD) in a format permitting data subject identification for no longer than is necessary for legitimate business purposes.	5	
Article 5.1(f)	N/A	processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').	Functional	subset of	Security of Personal Data (PD)	PRI-01.6	Mechanisms exist to ensure Personal Data (PD) is protected by logical and physical security safeguards that are sufficient and appropriately scoped to protect the confidentiality and integrity of the PD.	10	
Article 5.2	N/A	The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').	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 6	Lawfulness of processing	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 6.1	N/A	Processing shall be lawful only if and to the extent that at least one of the following applies: Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 6.1(a)	N/A	the data subject has given consent to the processing of his or her personal data for one or more specific purposes;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 6.1(b)	N/A	processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 6.1(c)	N/A	processing is necessary for compliance with a legal obligation to which the controller is subject;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 6.1(d)	N/A	processing is necessary in order to protect the vital interests of the data subject or of another natural person;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 6.1(e)	N/A	processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	

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 6.1(f)	N/A	processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 6.2	N/A	Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 6.3	N/A	The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 6.3(a)	N/A	Union law; or	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 6.3(b)	N/A	Member State law to which the controller is subject. The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific 4.5.2016 L 119/36 Official Journal of the European Union EN processing situations as provided for in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 6.4	N/A	Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 6.4(a)	N/A	any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 6.4(b)	N/A	the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 6.4(c)	N/A	the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 6.4(d)	N/A	the possible consequences of the intended further processing for data subjects;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 6.4(e)	N/A	he existence of appropriate safeguards, which may include encryption or pseudonymisation.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 7	Conditions for consent	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 7.1	N/A	Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.	Functional	subset of	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.	10	
Article 7.2	N/A	If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.	Functional	subset of	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.	10	
Article 7.3	N/A	The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.	Functional	equal	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).	10	
Article 7.4	N/A	When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 8	Conditions applicable to child's consent in relation to information society services	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 8.1	N/A	Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.	Functional	intersects with	Restrict Collection To Identified Purpose	PRI-04	Mechanisms exist to minimize the collection of Personal Data (PD) to only what is adequate, relevant and limited to the purposes identified in the data privacy notice, including protections against collecting PD from minors without appropriate parental or legal guardian consent.	5	
Article 8.1	N/A	Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.	Functional	intersects with	Authorized Agent	PRI-03.6	Mechanisms exist to allow data subjects to authorize another person or entity, acting on the data subject's behalf, to make Personal Data (PD) processing decisions.	3	
Article 8.2	N/A	The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.	Functional	intersects with	Authorized Agent	PRI-03.6	Mechanisms exist to allow data subjects to authorize another person or entity, acting on the data subject's behalf, to make Personal Data (PD) processing decisions.	3	
Article 8.3	N/A	Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 9	Processing of special categories of personal data	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 9.1	N/A	Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.	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 9.2	N/A	Paragraph 1 shall not apply if one of the following applies:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	

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 9.2(a)	N/A	the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;	Functional	subset of	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.	10	
Article 9.2(b)	N/A	processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;	Functional	intersects with	Authority To Collect, Process, Store & Share Personal Data (PD)	PRI-04.1	Mechanisms exist to determine and document the legal authority that permits the organization to collect, receive, process, store, transmit, update and/or share Personal Data (PD), either generally or in support of a specific business process.	5	
Article 9.2(c)	N/A	processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;	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 9.2(d)	N/A	processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;	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 9.2(e)	N/A	processing relates to personal data which are manifestly made public by the data subject;	Functional	intersects with	Authority To Collect, Process, Store & Share Personal Data (PD)	PRI-04.1	Mechanisms exist to determine and document the legal authority that permits the organization to collect, receive, process, store, transmit, update and/or share Personal Data (PD), either generally or in support of a specific business process.	5	
Article 9.2(f)	N/A	processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;	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 9.2(g)	N/A	processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;	Functional	intersects with	Authority To Collect, Process, Store & Share Personal Data (PD)	PRI-04.1	Mechanisms exist to determine and document the legal authority that permits the organization to collect, receive, process, store, transmit, update and/or share Personal Data (PD), either generally or in support of a specific business process.	5	
Article 9.2(h)	N/A	processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;	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 9.2(i)	N/A	processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;	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 9.2(j)	N/A	processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.	Functional	intersects with	Authority To Collect, Process, Store & Share Personal Data (PD)	PRI-04.1	Mechanisms exist to determine and document the legal authority that permits the organization to collect, receive, process, store, transmit, update and/or share Personal Data (PD), either generally or in support of a specific business process.	5	
Article 9.3	N/A	Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.	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 9.4	N/A	Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 10	Processing of personal data relating to criminal convictions and offences	Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.	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 11	Processing which does not require identification	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 11.1	N/A	If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 11.2	N/A	Where, in cases referred to in paragraph 1 of this Article, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 15 to 20 shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 12	Transparent information, communication and modalities for the exercise of the rights of the data subject	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 12.1	N/A	The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.	Functional	intersects with	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.	5	
Article 12.2	N/A	The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.	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	

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 12.3	N/A	The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by 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 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 12.4	N/A	If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.	Functional	intersects with	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to complaints, concerns or questions from authenticated data subjects about how the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes of their Personal Data (PD).	5	
Article 12.5	N/A	Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either: The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 12.5(a)	N/A	charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 12.5(b)	N/A	refuse to act on the request.	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 12.6	N/A	Without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of 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 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 12.7	N/A	The information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.	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.	3	
Article 12.8	N/A	The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of determining the information to be presented by the icons and the procedures for providing standardised icons.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 13	Information to be provided where personal data are collected from the data subject	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 13.1	N/A	Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 13.1(a)	N/A	the identity and the contact details of the controller and, where applicable, of the controller's representative;	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 13.1(b)	N/A	the contact details of the data protection officer, where applicable;	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	

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 13.1(c)	N/A	the purposes of the processing for which the personal data are intended as well as the legal basis for the 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 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 13.1(c)	N/A	the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;	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.	8	
Article 13.1(d)	N/A	where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;	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 13.1(e)	N/A	the recipients or categories of recipients of the personal data, if any;	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 13.1(e)	N/A	the recipients or categories of recipients of the personal data, if any;	Functional	intersects with	Personal Data Categories	PRI-05.7	Mechanisms exist to define and implement data handling and protection requirements for specific categories of sensitive Personal Data (PD).	3	
Article 13.2	N/A	where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.	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(a)	N/A	the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;	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(b)	N/A	the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;	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(c)	N/A	where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;	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	

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 13.2(d)	N/A	the right to lodge a complaint with a supervisory authority;	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(e)	N/A	whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such 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 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(f)	N/A	the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for 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 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 13.3	N/A	Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.	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 13.4	N/A	Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 14	Information to be provided where personal data have not been obtained from the data subject	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 14.1	N/A	Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 14.1(a)	N/A	the identity and the contact details of the controller and, where applicable, of the controller's representative;	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 14.1(b)	N/A	the contact details of the data protection officer, where applicable;	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	

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 14.1(c)	N/A	the purposes of the processing for which the personal data are intended as well as the legal basis for the 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 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 14.1(c)	N/A	the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;	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 14.1(d)	N/A	the categories of personal data concerned;	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 14.1(d)	N/A	the categories of personal data concerned;	Functional	intersects with	Personal Data Categories	PRI-05.7	Mechanisms exist to define and implement data handling and protection requirements for specific categories of sensitive Personal Data (PD).	3	
Article 14.1(e)	N/A	the recipients or categories of recipients of the personal data, if any;	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 14.1(f)	N/A	where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.	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 14.2	N/A	In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of 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 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 14.2(a)	N/A	the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;	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 14.2(b)	N/A	where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;	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	

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 14.2(c)	N/A	the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;	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 14.2(d)	N/A	where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;	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 14.2(e)	N/A	the right to lodge a complaint with a supervisory authority;	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 14.2(f)	N/A	from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;	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 14.2(g)	N/A	the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for 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 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 14.3	N/A	The controller shall provide the information referred to in paragraphs 1 and 2:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 14.3(a)	N/A	within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;	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 14.3(b)	N/A	if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or	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	

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 14.3(c)	N/A	if a disclosure to another recipient is envisaged, at the latest when the personal data are first 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 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 14.4	N/A	Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.	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 14.5	N/A	Paragraphs 1 to 4 shall not apply where and insofar as:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 14.5(a)	N/A	the data subject already has the information;	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 14.5(b)	N/A	the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 14.5(c)	N/A	obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 14.5(d)	N/A	where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 15	Right of access by the data subject	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 15.1	N/A	The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:	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 15.1(a)	N/A	the purposes of the 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 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 15.1(b)	N/A	the categories of personal data concerned;	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 15.1(c)	N/A	the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;	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 15.1(d)	N/A	where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that 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 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 15.1(e)	N/A	the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such 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 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 15.1(f)	N/A	the right to lodge a complaint with a supervisory authority;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 15.1(g)	N/A	where the personal data are not collected from the data subject, any available information as to their source;	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 15.1(h)	N/A	the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for 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 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 15.2	N/A	Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.	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 15.3	N/A	The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.	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 15.4	N/A	The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.	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 16	Right to rectification	The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.	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 17	Right to erasure (‘right to be forgotten’)	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 17.1	N/A	The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:	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 17.1	N/A	The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:	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 17.1(a)	N/A	the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;	Functional	intersects with	Right to Erasure	PRI-06.5	Mechanisms exist to maintain a process to erase a data subject's Personal Data (PD), in accordance with applicable laws, regulations and contractual obligations pertaining to the retention of their PD.	5	
Article 17.1(b)	N/A	the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;	Functional	intersects with	Right to Erasure	PRI-06.5	Mechanisms exist to maintain a process to erase a data subject's Personal Data (PD), in accordance with applicable laws, regulations and contractual obligations pertaining to the retention of their PD.	5	
Article 17.1(c)	N/A	the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);	Functional	intersects with	Right to Erasure	PRI-06.5	Mechanisms exist to maintain a process to erase a data subject's Personal Data (PD), in accordance with applicable laws, regulations and contractual obligations pertaining to the retention of their PD.	5	
Article 17.1(d)	N/A	the personal data have been unlawfully processed;	Functional	intersects with	Right to Erasure	PRI-06.5	Mechanisms exist to maintain a process to erase a data subject's Personal Data (PD), in accordance with applicable laws, regulations and contractual obligations pertaining to the retention of their PD.	5	
Article 17.1(e)	N/A	the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;	Functional	intersects with	Right to Erasure	PRI-06.5	Mechanisms exist to maintain a process to erase a data subject's Personal Data (PD), in accordance with applicable laws, regulations and contractual obligations pertaining to the retention of their PD.	5	
Article 17.1(f)	N/A	the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).	Functional	intersects with	Right to Erasure	PRI-06.5	Mechanisms exist to maintain a process to erase a data subject's Personal Data (PD), in accordance with applicable laws, regulations and contractual obligations pertaining to the retention of their PD.	5	
Article 17.2	N/A	Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.	Functional	intersects with	Right to Erasure	PRI-06.5	Mechanisms exist to maintain a process to erase a data subject's Personal Data (PD), in accordance with applicable laws, regulations and contractual obligations pertaining to the retention of their PD.	5	
Article 17.3	N/A	Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:	Functional	intersects with	Right to Erasure	PRI-06.5	Mechanisms exist to maintain a process to erase a data subject's Personal Data (PD), in accordance with applicable laws, regulations and contractual obligations pertaining to the retention of their PD.	5	
Article 17.3(a)	N/A	for exercising the right of freedom of expression and information;	Functional	intersects with	Right to Erasure	PRI-06.5	Mechanisms exist to maintain a process to erase a data subject's Personal Data (PD), in accordance with applicable laws, regulations and contractual obligations pertaining to the retention of their PD.	5	
Article 17.3(b)	N/A	for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;	Functional	intersects with	Right to Erasure	PRI-06.5	Mechanisms exist to maintain a process to erase a data subject's Personal Data (PD), in accordance with applicable laws, regulations and contractual obligations pertaining to the retention of their PD.	5	
Article 17.3(c)	N/A	for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);	Functional	intersects with	Right to Erasure	PRI-06.5	Mechanisms exist to maintain a process to erase a data subject's Personal Data (PD), in accordance with applicable laws, regulations and contractual obligations pertaining to the retention of their PD.	5	
Article 17.3(d)	N/A	for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or	Functional	intersects with	Right to Erasure	PRI-06.5	Mechanisms exist to maintain a process to erase a data subject's Personal Data (PD), in accordance with applicable laws, regulations and contractual obligations pertaining to the retention of their PD.	5	
Article 17.3(e)	N/A	for the establishment, exercise or defence of legal claims.	Functional	intersects with	Right to Erasure	PRI-06.5	Mechanisms exist to maintain a process to erase a data subject's Personal Data (PD), in accordance with applicable laws, regulations and contractual obligations pertaining to the retention of their PD.	5	
Article 18	Right to restriction of processing	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	

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 18.1	N/A	The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:	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 18.1(a)	N/A	the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;	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 18.1(b)	N/A	the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;	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 18.1(c)	N/A	the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;	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 18.1(d)	N/A	the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of 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 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 18.2	N/A	Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.	Functional	intersects with	Continued Use of Personal Data (PD)	PRI-03.9	Mechanisms exist to govern the continued use of Personal Data (PD) as it is collected, received, processed, stored, transmitted and/or shared until: (1) Disposal of PD occurs when there is no longer a legitimate business purpose; (2) Disposal of PD occurs when the data retention timeline for the use case is met; and/or (3) Continued use of PD is prohibited upon withdrawal of data subject consent.	5	
Article 18.3	N/A	A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.	Functional	intersects with	Communicating Processing Changes	PRI-03.11	Mechanisms exist to notify data subjects of processing changes affecting their Personal Data (PD), including: (1) Erasure of PD; (2) Remediation of incorrect PD; and/or (3) Processing restrictions affecting their PD.	5	
Article 19	Notification obligation regarding rectification or erasure of personal data or restriction of processing	The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.	Functional	intersects with	Communicating Processing Changes	PRI-03.11	Mechanisms exist to notify data subjects of processing changes affecting their Personal Data (PD), including: (1) Erasure of PD; (2) Remediation of incorrect PD; and/or (3) Processing restrictions affecting their PD.	5	
Article 20	Right to data portability	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 20.1	N/A	The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:	Functional	intersects with	Data Portability	PRI-06.6	Mechanisms exist to format exports of Personal Data (PD) in a structured, machine-readable format that allows data subjects to transfer their PD to another controller without hindrance.	8	
Article 20.1	N/A	The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:	Functional	intersects with	Personal Data (PD) Exports	PRI-06.7	Mechanisms exist to export a data subject's available Personal Data (PD) in a readily usable format, upon an authenticated request.	8	
Article 20.1(a)	N/A	the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 20.1(b)	N/A	the processing is carried out by automated means.	Functional	intersects with	Personal Data (PD) Exports	PRI-06.7	Mechanisms exist to export a data subject's available Personal Data (PD) in a readily usable format, upon an authenticated request.	8	
Article 20.2	N/A	In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	

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 20.3	N/A	The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 20.4	N/A	The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 21	Right to object	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 21.1	N/A	The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.	Functional	subset of	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.	10	
Article 21.2	N/A	Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.	Functional	subset of	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.	10	
Article 21.3	N/A	Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.	Functional	subset of	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.	10	
Article 21.4	N/A	At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.	Functional	subset of	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.	10	
Article 21.5	N/A	In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.	Functional	subset of	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.	10	
Article 21.6	N/A	Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.	Functional	subset of	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.	10	
Article 22	Automated individual decision-making, including profiling	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 22.1	N/A	The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 22.2	N/A	Paragraph 1 shall not apply if the decision:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 22.2(a)	N/A	is necessary for entering into, or performance of, a contract between the data subject and a data controller;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 22.2(b)	N/A	is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 22.2(c)	N/A	is based on the data subject's explicit consent.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 22.3	N/A	In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 22.4	N/A	Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 23	Restrictions	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 23.1	N/A	Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 23.1(a)	N/A	national security;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 23.1(b)	N/A	defence;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 23.1(c)	N/A	public security;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 23.1(d)	N/A	the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 23.1(e)	N/A	other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 23.1(f)	N/A	the protection of judicial independence and judicial proceedings;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 23.1(g)	N/A	the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 23.1(h)	N/A	a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 23.1(i)	N/A	the protection of the data subject or the rights and freedoms of others;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 23.1(j)	N/A	the enforcement of civil law claims.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 23.2	N/A	In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, as to:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 23.2(a)	N/A	the purposes of the processing or categories of processing;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 23.2(b)	N/A	the categories of personal data;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 23.2(c)	N/A	the scope of the restrictions introduced;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 23.2(d)	N/A	the safeguards to prevent abuse or unlawful access or transfer;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 23.2(e)	N/A	the specification of the controller or categories of controllers;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	

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 23.2(f)	N/A	the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 23.2(g)	N/A	the risks to the rights and freedoms of data subjects; and	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 23.2(h)	N/A	the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 24	Responsibility of the controller	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 24.1	N/A	Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.	Functional	subset of	Security of Personal Data (PD)	PRI-01.6	Mechanisms exist to ensure Personal Data (PD) is protected by logical and physical security safeguards that are sufficient and appropriately scoped to protect the confidentiality and integrity of the PD.	10	
Article 24.2	N/A	Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.	Functional	subset of	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	10	
Article 24.3	N/A	Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 25	Data protection by design and by default	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 25.1	N/A	Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.	Functional	subset of	Security of Personal Data (PD)	PRI-01.6	Mechanisms exist to ensure Personal Data (PD) is protected by logical and physical security safeguards that are sufficient and appropriately scoped to protect the confidentiality and integrity of the PD.	10	
Article 25.2	N/A	The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.	Functional	subset of	Security of Personal Data (PD)	PRI-01.6	Mechanisms exist to ensure Personal Data (PD) is protected by logical and physical security safeguards that are sufficient and appropriately scoped to protect the confidentiality and integrity of the PD.	10	
Article 25.3	N/A	An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 26	Joint controllers	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 26.1	N/A	Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 26.2	N/A	The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 26.3	N/A	Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 27	Representatives of controllers or processors not established in the Union	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 27.1	N/A	Where Article 3(2) applies, the controller or the processor shall designate in writing a representative in the Union.	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.	8	
Article 27.2	N/A	The obligation laid down in paragraph 1 of this Article shall not apply to:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 27.2(a)	N/A	processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 27.2(b)	N/A	a public authority or body.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 27.3	N/A	The representative shall be established in one of the Member States where the data subjects, whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, are.	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.	8	
Article 27.4	N/A	The representative shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this Regulation.	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.	8	
Article 27.5	N/A	The designation of a representative by the controller or processor shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves.	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.	8	
Article 28	Processor	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 28.1	N/A	Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.	Functional	intersects with	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
Article 28.2	N/A	The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.	Functional	intersects with	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
Article 28.3	N/A	Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor: With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.	Functional	intersects with	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
Article 28.3(a)	N/A	processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;	Functional	intersects with	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	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 28.3(b)	N/A	ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;	Functional	intersects with	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
Article 28.3(c)	N/A	takes all measures required pursuant to Article 32;	Functional	intersects with	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
Article 28.3(d)	N/A	respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;	Functional	intersects with	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
Article 28.3(e)	N/A	taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;	Functional	intersects with	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
Article 28.3(f)	N/A	assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;	Functional	intersects with	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
Article 28.3(g)	N/A	at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;	Functional	intersects with	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
Article 28.3(h)	N/A	makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.	Functional	intersects with	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
Article 28.4	N/A	Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.	Functional	intersects with	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
Article 28.5	N/A	Adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article.	Functional	intersects with	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
Article 28.6	N/A	Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 3 and 4 of this Article may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 7 and 8 of this Article, including when they are part of a certification granted to the controller or processor pursuant to Articles 42 and 43.	Functional	intersects with	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
Article 28.7	N/A	The Commission may lay down standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the examination procedure referred to in Article 93(2).	Functional	intersects with	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
Article 28.8	N/A	A supervisory authority may adopt standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the consistency mechanism referred to in Article 63.	Functional	intersects with	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
Article 28.9	N/A	The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form.	Functional	intersects with	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
Article 28.10	N/A	Without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.	Functional	intersects with	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
Article 29	Processing under the authority of the controller or processor	The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.	Functional	intersects with	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
Article 30	Records of processing activities	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 30.1	N/A	Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:	Functional	intersects with	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.	5	
Article 30.1(a)	N/A	the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;	Functional	intersects with	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.	5	
Article 30.1(b)	N/A	the purposes of the processing;	Functional	intersects with	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.	5	
Article 30.1(c)	N/A	a description of the categories of data subjects and of the categories of personal data;	Functional	intersects with	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.	5	
Article 30.1(d)	N/A	the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;	Functional	intersects with	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.	5	
Article 30.1(e)	N/A	where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;	Functional	intersects with	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.	5	
Article 30.1(f)	N/A	where possible, the envisaged time limits for erasure of the different categories of data;	Functional	intersects with	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.	5	
Article 30.1(g)	N/A	where possible, a general description of the technical and organisational security measures referred to in Article 32(1).	Functional	intersects with	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.	5	
Article 30.2	N/A	Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:	Functional	intersects with	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.	5	
Article 30.2(a)	N/A	the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;	Functional	intersects with	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.	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 30.2(b)	N/A	the categories of processing carried out on behalf of each controller;	Functional	intersects with	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.	5	
Article 30.2(c)	N/A	where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;	Functional	intersects with	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.	5	
Article 30.2(d)	N/A	where possible, a general description of the technical and organisational security measures referred to in Article 32(1).	Functional	intersects with	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.	5	
Article 30.3	N/A	The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.	Functional	intersects with	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.	5	
Article 30.4	N/A	The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.	Functional	intersects with	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.	5	
Article 30.5	N/A	The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 31	Cooperation with the supervisory authority	The controller and the processor and, where applicable, their representatives, shall cooperate, on request, with the supervisory authority in the performance of its tasks.	Functional	intersects with	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.	8	
Article 32	Security of processing	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 32.1	N/A	Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:	Functional	subset of	Security of Personal Data (PD)	PRI-01.6	Mechanisms exist to ensure Personal Data (PD) is protected by logical and physical security safeguards that are sufficient and appropriately scoped to protect the confidentiality and integrity of the PD.	10	
Article 32.1(a)	N/A	the pseudonymisation and encryption of personal data;	Functional	intersects with	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	8	
Article 32.1(a)	N/A	the pseudonymisation and encryption of personal data;	Functional	intersects with	Security of Personal Data (PD)	PRI-01.6	Mechanisms exist to ensure Personal Data (PD) is protected by logical and physical security safeguards that are sufficient and appropriately scoped to protect the confidentiality and integrity of the PD.	8	
Article 32.1(b)	N/A	the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;	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 32.1(c)	N/A	the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
Article 32.1(d)	N/A	a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.	Functional	intersects with	Cybersecurity & Data Protection Controls Oversight	CPL-02	Mechanisms exist to provide a cybersecurity & data protection controls oversight function that reports to the organization's executive leadership.	5	
Article 32.1(d)	N/A	a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.	Functional	intersects with	Periodic Audits	CPL-02.2	Mechanisms exist to conduct periodic audits of cybersecurity & data protection controls to evaluate conformity with the organization's documented policies, standards and procedures.	5	
Article 32.2	N/A	In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.	Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
Article 32.3	N/A	Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 32.4	N/A	The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.	Functional	intersects with	Position Categorization	HRS-02	Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions.	8	
Article 32.4	N/A	The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.	Functional	intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	8	
Article 32.4	N/A	The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.	Functional	intersects with	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce a Role-Based Access Control (RBAC) policy over users and resources that applies need-to-know and fine-grained access control for sensitive/regulated data access.	8	
Article 33	Notification of a personal data breach to the supervisory authority	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 33.1	N/A	In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.	Functional	subset of	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.	10	
Article 33.1	N/A	In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.	Functional	intersects with	Cyber Incident Reporting for Sensitive Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	8	
Article 33.2	N/A	The processor shall notify the controller without undue delay after becoming aware of a personal data breach.	Functional	intersects with	Cyber Incident Reporting for Sensitive Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	5	
Article 33.3	N/A	The notification referred to in paragraph 1 shall at least:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 33.3(a)	N/A	describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;	Functional	intersects with	Cyber Incident Reporting for Sensitive Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	5	
Article 33.3(b)	N/A	communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;	Functional	intersects with	Cyber Incident Reporting for Sensitive Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	5	
Article 33.3(c)	N/A	describe the likely consequences of the personal data breach;	Functional	intersects with	Cyber Incident Reporting for Sensitive Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	5	
Article 33.3(d)	N/A	describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.	Functional	intersects with	Cyber Incident Reporting for Sensitive Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	5	
Article 33.4	N/A	Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.	Functional	intersects with	Cyber Incident Reporting for Sensitive Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	5	
Article 33.5	N/A	The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.	Functional	intersects with	Situational Awareness For Incidents	IRO-09	Mechanisms exist to document, monitor and report the status of cybersecurity & data privacy incidents to internal stakeholders all the way through the resolution of the incident.	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 34	Communication of a personal data breach to the data subject	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 34.1	N/A	When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.	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	
Article 34.2	N/A	The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).	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	
Article 34.3	N/A	The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 34.3(a)	N/A	the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 34.3(b)	N/A	the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 34.3(c)	N/A	it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 34.4	N/A	If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 35	Data protection impact assessment	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 35.1	N/A	Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.	Functional	subset of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	
Article 35.2	N/A	The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.	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 35.3	N/A	A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 35.3(a)	N/A	a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;	Functional	subset of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	
Article 35.3(b)	N/A	processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or	Functional	subset of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	
Article 35.3(c)	N/A	a systematic monitoring of a publicly accessible area on a large scale.	Functional	subset of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	
Article 35.4	N/A	The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 35.5	N/A	The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 35.6	N/A	Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 35.7	N/A	The assessment shall contain at least:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 35.7(a)	N/A	a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;	Functional	subset of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	
Article 35.7(b)	N/A	an assessment of the necessity and proportionality of the processing operations in relation to the purposes;	Functional	subset of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	
Article 35.7(c)	N/A	an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and	Functional	subset of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	
Article 35.7(d)	N/A	the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.	Functional	subset of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	
Article 35.8	N/A	Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.	Functional	subset of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	
Article 35.9	N/A	Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.	Functional	subset of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	
Article 35.10	N/A	Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 35.11	N/A	Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.	Functional	subset of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	
Article 36	Prior consultation	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 36.1	N/A	The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.	Functional	subset of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
Article 36.2	N/A	Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 1 would infringe this Regulation, in particular where the controller has insufficiently identified or mitigated the risk, the supervisory authority shall, within period of up to eight weeks of receipt of the request for consultation, provide written advice to the controller and, where applicable to the processor, and may use any of its powers referred to in Article 58. That period may be extended by six weeks, taking into account the complexity of the intended processing. The supervisory authority shall inform the controller and, where applicable, the processor, of any such extension within one month of receipt of the request for consultation together with the reasons for the delay. Those periods may be suspended until the supervisory authority has obtained information it has requested for the purposes of the consultation.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 36.3	N/A	When consulting the supervisory authority pursuant to paragraph 1, the controller shall provide the supervisory authority with:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 36.3(a)	N/A	where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 36.3(b)	N/A	the purposes and means of the intended processing;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 36.3(c)	N/A	the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 36.3(d)	N/A	where applicable, the contact details of the data protection officer;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 36.3(e)	N/A	the data protection impact assessment provided for in Article 35; and	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 36.3(f)	N/A	any other information requested by the supervisory authority.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 36.4	N/A	Member States shall consult the supervisory authority during the preparation of a proposal for a legislative measure to be adopted by a national parliament, or of a regulatory measure based on such a legislative measure, which relates to processing.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 36.5	N/A	Notwithstanding paragraph 1, Member State law may require controllers to consult with, and obtain prior authorisation from, the supervisory authority in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 37	Designation of the data protection officer	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 37.1	N/A	The controller and the processor shall designate a data protection officer in any case where:	Functional	subset of	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.	10	
Article 37.1(a)	N/A	the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;	Functional	subset of	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.	10	
Article 37.1(b)	N/A	the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or	Functional	subset of	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.	10	
Article 37.1(c)	N/A	the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.	Functional	subset of	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.	10	
Article 37.2	N/A	A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.	Functional	subset of	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.	10	
Article 37.3	N/A	Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.	Functional	subset of	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.	10	
Article 37.4	N/A	In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors.	Functional	subset of	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.	10	
Article 37.5	N/A	The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.	Functional	subset of	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.	10	
Article 37.6	N/A	The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.	Functional	subset of	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.	10	
Article 37.7	N/A	The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.	Functional	subset of	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.	10	
Article 38	Position of the data protection officer	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 38.1	N/A	The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.	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 38.2	N/A	The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.	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 38.3	N/A	The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.	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 38.4	N/A	Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.	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 38.5	N/A	The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State 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 38.6	N/A	The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.	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 39	Tasks of the data protection officer	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 39.1	N/A	The data protection officer shall have at least the following tasks:	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 39.1(a)	N/A	to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;	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 39.1(b)	N/A	to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;	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	

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 39.1(c)	N/A	to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;	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 39.1(d)	N/A	to cooperate with the supervisory authority;	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 39.1(e)	N/A	to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.	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 39.2	N/A	The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.	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 40	Codes of conduct	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 40.1	N/A	The Member States, the supervisory authorities, the Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 40.2	N/A	Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 40.2(a)	N/A	fair and transparent processing;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 40.2(b)	N/A	the legitimate interests pursued by controllers in specific contexts;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 40.2(c)	N/A	the collection of personal data;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 40.2(d)	N/A	the pseudonymisation of personal data;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 40.2(e)	N/A	the information provided to the public and to data subjects;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 40.2(f)	N/A	the exercise of the rights of data subjects;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 40.2(g)	N/A	the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 40.2(h)	N/A	the measures and procedures referred to in Articles 24 and 25 and the measures to ensure security of processing referred to in Article 32;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 40.2(i)	N/A	the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 40.2(j)	N/A	the transfer of personal data to third countries or international organisations; or	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 40.2(k)	N/A	out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects pursuant to Articles 77 and 79.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 40.3	N/A	In addition to adherence by controllers or processors subject to this Regulation, codes of conduct approved pursuant to paragraph 5 of this Article and having general validity pursuant to paragraph 9 of this Article may also be adhered to by controllers or processors that are not subject to this Regulation pursuant to Article 3 in order to provide appropriate safeguards within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (e) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards including with regard to the rights of data subjects.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 40.4	N/A	A code of conduct referred to in paragraph 2 of this Article shall contain mechanisms which enable the body referred to in Article 41(1) to carry out the mandatory monitoring of compliance with its provisions by the controllers or processors which undertake to apply it, without prejudice to the tasks and powers of supervisory authorities competent pursuant to Article 55 or 56.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 40.5	N/A	Associations and other bodies referred to in paragraph 2 of this Article which intend to prepare a code of conduct or to amend or extend an existing code shall submit the draft code, amendment or extension to the supervisory authority which is competent pursuant to Article 55. The supervisory authority shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation and shall approve that draft code, amendment or extension if it finds that it provides sufficient appropriate safeguards.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 40.6	N/A	Where the draft code, or amendment or extension is approved in accordance with paragraph 5, and where the code of conduct concerned does not relate to processing activities in several Member States, the supervisory authority shall register and publish the code.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 40.7	N/A	Where a draft code of conduct relates to processing activities in several Member States, the supervisory authority which is competent pursuant to Article 55 shall, before approving the draft code, amendment or extension, submit it in the procedure referred to in Article 63 to the Board which shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation or, in the situation referred to in paragraph 3 of this Article, provides appropriate safeguards.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 40.8	N/A	Where the opinion referred to in paragraph 7 confirms that the draft code, amendment or extension complies with this Regulation, or, in the situation referred to in paragraph 3, provides appropriate safeguards, the Board shall submit its opinion to the Commission.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 40.9	N/A	The Commission may, by way of implementing acts, decide that the approved code of conduct, amendment or extension submitted to it pursuant to paragraph 8 of this Article have general validity within the Union. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 40.10	N/A	The Commission shall ensure appropriate publicity for the approved codes which have been decided as having general validity in accordance with paragraph 9.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 40.11	N/A	The Board shall collate all approved codes of conduct, amendments and extensions in a register and shall make them publicly available by way of appropriate means.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 41	N/A	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 42	N/A	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 43	N/A	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 44	General principle for transfers	Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.	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 45	Transfers on the basis of an adequacy decision	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 45.1	N/A	A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.	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 45.1	N/A	A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.	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.	8	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
Article 45.2	N/A	When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 45.2(a)	N/A	the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 45.2(b)	N/A	the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 45.2(c)	N/A	the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 45.3	N/A	The Commission, after assessing the adequacy of the level of protection, may decide, by means of implementing act, that a third country, a territory or one or more specified sectors within a third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2 of this Article. The implementing act shall provide for a mechanism for a periodic review, at least every four years, which shall take into account all relevant developments in the third country or international organisation. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority or authorities referred to in point (b) of paragraph 2 of this Article. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 93(2).	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 45.4	N/A	The Commission shall, on an ongoing basis, monitor developments in third countries and international organisations that could affect the functioning of decisions adopted pursuant to paragraph 3 of this Article and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 45.5	N/A	The Commission shall, where available information reveals, in particular following the review referred to in paragraph 3 of this Article, that a third country, a territory or one or more specified sectors within a third country, or an international organisation no longer ensures an adequate level of protection within the meaning of paragraph 2 of this Article, to the extent necessary, repeal, amend or suspend the decision referred to in paragraph 3 of this Article by means of implementing acts without retro-active effect. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2). On duly justified imperative grounds of urgency, the Commission shall adopt immediately applicable implementing acts in accordance with the procedure referred to in Article 93(3).	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 45.6	N/A	The Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the decision made pursuant to paragraph 5.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 45.7	N/A	A decision pursuant to paragraph 5 of this Article is without prejudice to transfers of personal data to the third country, a territory or one or more specified sectors within that third country, or the international organisation in question pursuant to Articles 46 to 49.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 45.8	N/A	The Commission shall publish in the Official Journal of the European Union and on its website a list of the third countries, territories and specified sectors within a third country and international organisations for which it has decided that an adequate level of protection is or is no longer ensured.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 45.9	N/A	Decisions adopted by the Commission on the basis of Article 25(6) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by a Commission Decision adopted in accordance with paragraph 3 or 5 of this Article.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 46	Transfers subject to appropriate safeguards	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 46.1	N/A	In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.	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 46.1	N/A	In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.	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.	8	
Article 46.2	N/A	The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:	Functional	intersects with	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.	5	
Article 46.2(a)	N/A	a legally binding and enforceable instrument between public authorities or bodies;	Functional	intersects with	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.	5	
Article 46.2(b)	N/A	binding corporate rules in accordance with Article 47;	Functional	equal	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 46.2(c)	N/A	standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 46.2(d)	N/A	standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 46.2(e)	N/A	an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 46.2(f)	N/A	an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 46.3	N/A	Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 46.3(a)	N/A	contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or	Functional	subset of	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	10	
Article 46.3(b)	N/A	provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 46.4	N/A	The supervisory authority shall apply the consistency mechanism referred to in Article 63 in the cases referred to in paragraph 3 of this Article.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	

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 46.5	N/A	Authorisations by a Member State or supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid until amended, replaced or repealed, if necessary, by that supervisory authority. Decisions adopted by the Commission on the basis of Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed, if necessary, by a Commission Decision adopted in accordance with paragraph 2 of this Article.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 47	Binding corporate rules	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 47.1	N/A	The competent supervisory authority shall approve binding corporate rules in accordance with the consistency mechanism set out in Article 63, provided that they:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 47.1(a)	N/A	are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 47.1(b)	N/A	expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 47.1(c)	N/A	fulfil the requirements laid down in paragraph 2.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 47.2	N/A	The binding corporate rules referred to in paragraph 1 shall specify at least:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 47.2(a)	N/A	the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 47.2(b)	N/A	the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 47.2(c)	N/A	their legally binding nature, both internally and externally;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 47.2(d)	N/A	the application of the general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 47.2(e)	N/A	the rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling in accordance with Article 22, the right to lodge a complaint with the competent supervisory authority and before the competent courts of the Member States in accordance with Article 79, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 47.2(f)	N/A	the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member concerned not established in the Union; the controller or the processor shall be exempt from that liability, in whole or in part, only if it proves that that member is not responsible for the event giving rise to the damage;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 47.2(g)	N/A	how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in addition to Articles 13 and 14;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 47.2(h)	N/A	the tasks of any data protection officer designated in accordance with Article 37 or any other person or entity in charge of the monitoring compliance with the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 47.2(i)	N/A	the complaint procedures;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 47.2(j)	N/A	the mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the binding corporate rules. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. Results of such verification should be communicated to the person or entity referred to in point (h) and to the board of the controlling undertaking of a group of undertakings, or of the group of enterprises engaged in a joint economic activity, and should be available upon request to the competent supervisory authority;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 47.2(k)	N/A	the mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authority;	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 47.2(l)	N/A	the cooperation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, or group of enterprises engaged in a joint economic activity, in particular by making available to the supervisory authority the results of verifications of the measures referred to in point (j);	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 47.2(m)	N/A	the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 47.2(n)	N/A	the appropriate data protection training to personnel having permanent or regular access to personal data.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 47.3	N/A	The Commission may specify the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 48	Transfers or disclosures not authorised by Union law	Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 49	Derogations for specific situations	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 49.1	N/A	In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions: Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.	Functional	intersects with	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.	5	
Article 49.1(a)	N/A	the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;	Functional	intersects with	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.	5	
Article 49.1(b)	N/A	the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;	Functional	intersects with	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.	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 49.1(c)	N/A	the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;	Functional	intersects with	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.	5	
Article 49.1(d)	N/A	the transfer is necessary for important reasons of public interest;	Functional	intersects with	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.	5	
Article 49.1(e)	N/A	the transfer is necessary for the establishment, exercise or defence of legal claims;	Functional	intersects with	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.	5	
Article 49.1(f)	N/A	the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;	Functional	intersects with	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.	5	
Article 49.1(g)	N/A	the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.	Functional	intersects with	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.	5	
Article 49.2	N/A	A transfer pursuant to point (g) of the first subparagraph of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.	Functional	intersects with	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.	5	
Article 49.3	N/A	Points (a), (b) and (c) of the first subparagraph of paragraph 1 and the second subparagraph thereof shall not apply to activities carried out by public authorities in the exercise of their public powers.	Functional	intersects with	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.	5	
Article 49.4	N/A	The public interest referred to in point (d) of the first subparagraph of paragraph 1 shall be recognised in Union law or in the law of the Member State to which the controller is subject.	Functional	intersects with	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.	5	
Article 49.5	N/A	In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation. Member States shall notify such provisions to the Commission.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 49.6	N/A	The controller or processor shall document the assessment as well as the suitable safeguards referred to in the second subparagraph of paragraph 1 of this Article in the records referred to in Article 30.	Functional	intersects with	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.	5	
Article 50	International cooperation for the protection of personal data	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 51	Supervisory authority	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 52	Independence	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 53	General conditions for the members of the supervisory authority	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 54	Rules on the establishment of the supervisory authority	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 55	Competence	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 56	Competence of the lead supervisory authority	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 57	Tasks	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 58	Powers	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 59	Activity reports	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 60	Cooperation between the lead supervisory authority and the other supervisory authorities concerned	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 61	Mutual assistance	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 62	Joint operations of supervisory authorities	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 63	Consistency mechanism	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 64	Opinion of the Board	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 65	Dispute resolution by the Board	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 66	Urgency procedure	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 67	Exchange of information	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 68	European Data Protection Board	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 69	Independence	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 70	Tasks of the Board	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 71	Reports	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 72	Procedure	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 73	Chair	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 74	Tasks of the Chair	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 75	Secretariat	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 76	Confidentiality	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 77	Right to lodge a complaint with a supervisory authority	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 78	Right to an effective judicial remedy against a supervisory authority	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 79	Right to an effective judicial remedy against a controller or processor	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 80	Representation of data subjects	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 81	Suspension of proceedings	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 82	Right to compensation and liability	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 83	General conditions for imposing administrative fines	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 84	Penalties	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 85	Processing and freedom of expression and information	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 86	Processing and public access to official documents	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 87	Processing of the national identification number	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 88	Processing in the context of employment	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 89	Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	

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 89.1	N/A	Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 89.2	N/A	Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 89.3	N/A	Where personal data are processed for archiving purposes in the public interest, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18, 19, 20 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 89.4	N/A	Where processing referred to in paragraphs 2 and 3 serves at the same time another purpose, the derogations shall apply only to processing for the purposes referred to in those paragraphs.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 90	Obligations of secrecy	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 91	Existing data protection rules of churches and religious associations	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 92	Exercise of the delegation	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 93	Committee procedure	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 94	Repeal of Directive 95/46/EC	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 95	Relationship with Directive 2002/58/EC	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 96	Relationship with previously concluded Agreements	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 97	Commission reports	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 98	Review of other Union legal acts on data protection	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 99	Entry into force and application	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 100	N/A	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 101	N/A	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 102	N/A	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
Article 103	N/A	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	