NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference document: Secure Controls Framework (SCF) version 2026.1
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: American Institute of Certified Public Accountants (AICPA) Privacy Management Framework (PMF) (2020)
Focal Document URL: https://www.aicpa-cima.com/resources/download/privacy-management-framework
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-general-aicpa-pmf-2020.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
M1.0	Management	The entity has defined and formally documented data and information privacy policies and procedures for PI collection, usage and processing that are consistent with the entity's objectives related to privacy.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	EU GDPR Articles 5, 6, 24, 27, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40
M1.0	Management	The entity has defined and formally documented data and information privacy policies and procedures for PI collection, usage and processing that are consistent with the entity's objectives related to privacy.	Functional	Intersects With	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.	8	EU GDPR Articles 5, 6, 24, 27, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40
M1.0-POF1	Agreement, notice and communication	The entity has formal agreements, provides notices and formally communicates with data subjects about its privacy practices to meet the entity's objectives related to privacy. Refer to Component N2.0.	Functional	Intersects With	Dissemination of Data Privacy Program Information	PRI-01.3	Mechanisms exist to: (1) Ensure that the public has access to information about organizational data privacy activities and can communicate with its Chief Privacy Officer (CPO) or similar role; (2) Ensure that organizational data privacy practices are publicly available through organizational websites or document repositories; (3) Utilize publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to data privacy office(s) regarding data privacy practices; and (4) Inform data subjects when changes are made to the privacy notice and the nature of such changes.	8	
M1.0-POF1	Agreement, notice and communication	The entity has formal agreements, provides notices and formally communicates with data subjects about its privacy practices to meet the entity's objectives related to privacy. Refer to Component N2.0.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations; (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
M1.0-POF2	Collection and creation	The entity has defined policies and procedures for collecting and creating a data subject's PI. Refer to Component C3.0.	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.	8	
M1.0-POF2	Collection and creation	The entity has defined policies and procedures for collecting and creating a data subject's PI. Refer to Component C3.0.	Functional	Intersects With	Personal Data (PD) Collection Methods	PRI-04.7	Mechanisms exist to ensure that Personal Data (PD) collection methods are: (1) In accordance with applicable statutory and/or regulatory requirements; (2) Appropriate for the circumstances of the data subject; (3) Unambiguous; and (4) Secure.	5	
M1.0-POF2	Collection and creation	The entity has defined policies and procedures for collecting and creating a data subject's PI. Refer to Component C3.0.	Functional	Intersects With	Authority To Collect, Process, Store & Share Personal Data (PD)	PRI-04.1	Mechanisms exist to determine and document the legal authority that permits the organization to collect, receive, process, store, transmit, share, update and/or dispose Personal Data (PD), either generally or in support of a specific business process.	3	
M1.0-POF3	Use, retention and disposal	The entity has policies and procedures for handling PI to achieve the stated purposes and needs for which the PI was initially collected. Refer to Component U4.0.	Functional	Intersects With	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to: (1) The purpose(s) originally collected, consistent with the data privacy notice(s); (2) What is authorized by the data subject, or authorized agent; and (3) What is consistent with applicable laws, regulations and contractual obligations.	8	
M1.0-POF4	Access	The entity has policies and procedures for viewing, inspecting, accessing and modifying PI. Refer to Component A5.0.	Functional	Intersects With	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	8	
M1.0-POF4	Access	The entity has policies and procedures for viewing, inspecting, accessing and modifying PI. Refer to Component A5.0.	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is processed and/or stored.	8	
M1.0-POF4	Access	The entity has policies and procedures for viewing, inspecting, accessing and modifying PI. Refer to Component A5.0.	Functional	Intersects With	Defining Access Authorizations for Sensitive / Regulated Data	DCH-01.4	Mechanisms exist to explicitly define authorizations for specific individuals and/or roles for logical and /or physical access to sensitive/regulated data.	8	
M1.0-POF4	Access	The entity has policies and procedures for viewing, inspecting, accessing and modifying PI. Refer to Component A5.0.	Functional	Intersects With	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	8	
M1.0-POF5	Disclosure to third parties	The entity has policies and procedures for disclosing and transmitting PI to external third-party individuals and organizations not under the direct management or control of the entity. Refer to Component D6.0.	Functional	Intersects With	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	8	
M1.0-POF5	Disclosure to third parties	The entity has policies and procedures for disclosing and transmitting PI to external third-party individuals and organizations not under the direct management or control of the entity. Refer to Component D6.0.	Functional	Intersects With	Limiting Personal Data (PD) Disclosures	PRI-01.7	Mechanisms exist to limit the disclosure of Personal Data (PD) to authorized parties for the sole purpose for which the PD was obtained.	8	
M1.0-POF6	Security for privacy	The entity has policies and procedures for protecting the integrity of PI during initial and subsequent collection, creation, usage, processing, alteration, adaptation, re-organization, storage, destruction and erasure. Refer to Component S7.0.	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	
M1.0-POF7	Data quality and integrity	The entity has a process for preserving and periodically re-validating the quality and integrity of PI and verifying (e.g., confirming with data subjects) its continued accuracy, completeness and correctness. Refer to Component Q8.0.	Functional	Intersects With	Data Quality Operations	DCH-22	Mechanisms exist to check for Redundant, Obsolete/Outdated, Toxic or Trivial (ROTT) data to ensure the accuracy, relevance, timeliness, impact, completeness and de-identification of information throughout the information lifecycle.	8	
M1.0-POF7	Data quality and integrity	The entity has a process for preserving and periodically re-validating the quality and integrity of PI and verifying (e.g., confirming with data subjects) its continued accuracy, completeness and correctness. Refer to Component Q8.0.	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.	8	
M1.0-POF8	Monitoring and enforcement	The entity has processes for assuring adherence to information privacy policies and procedures through ongoing and separate evaluations. Refer to Component M9.0.	Functional	Subset Of	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	10	
M1.2	N/A	The entity has implemented a policy governance and accountability process that defines and formally documents policies and procedures for information privacy that are consistent with the entity's objectives related to privacy.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
M1.2	N/A	The entity has implemented a policy governance and accountability process that defines and formally documents policies and procedures for information privacy that are consistent with the entity's objectives related to privacy.	Functional	Intersects With	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.	8	
M1.2-POF1	Responsibility and authority	The entity has an overall governance and legal structure that defines and establishes responsibility and authority for the entity's oversight processes, policy setting and ongoing monitoring activities	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	8	EU GDPR Articles, 27 (1); 37 (1), (2), (3), (4), (6); 38 (1), (3); 39 (1), (2)
M1.2-POF1	Responsibility and authority	The entity has an overall governance and legal structure that defines and establishes responsibility and authority for the entity's oversight processes, policy setting and ongoing monitoring activities	Functional	Intersects With	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5	EU GDPR Articles, 27 (1); 37 (1), (2), (3), (4), (6); 38 (1), (3); 39 (1), (2)
M1.2-POF1	Responsibility and authority	The entity has an overall governance and legal structure that defines and establishes responsibility and authority for the entity's oversight processes, policy setting and ongoing monitoring activities	Functional	Intersects With	Authoritative Chain of Command	GOV-04.2	Mechanisms exist to establish an authoritative chain of command with clear lines of communication to remove ambiguity from individuals and teams related to managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5	EU GDPR Articles, 27 (1); 37 (1), (2), (3), (4), (6); 38 (1), (3); 39 (1), (2)
M1.2-POF1	Responsibility and authority	The entity has an overall governance and legal structure that defines and establishes responsibility and authority for the entity's oversight processes, policy setting and ongoing monitoring activities	Functional	Intersects With	Chief Privacy Officer (CPO)	PRI-01.1	Mechanisms exist to appoints a Chief Privacy Officer (CPO) or similar role, with the authority, mission, accountability and resources to coordinate, develop and implement, applicable data privacy requirements and manage data privacy risks through the organization-wide data privacy program.	8	EU GDPR Articles, 27 (1); 37 (1), (2), (3), (4), (6); 38 (1), (3); 39 (1), (2)
M1.2-POF2	Established accountability	The entity has a governance and legal structure that establishes accountability for information privacy policy creation, oversight, monitoring and compliance.	Functional	Subset Of	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	10	Article 24 (2)
M1.2-POF3	Privacy awareness and training	The entity provides a privacy awareness program about its privacy policies and related matters, and provides specific training for selected personnel depending on their roles and responsibilities.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	8	
M1.2-POF3	Privacy awareness and training	The entity provides a privacy awareness program about its privacy policies and related matters, and provides specific training for selected personnel depending on their roles and responsibilities.	Functional	Intersects With	User Awareness	HRS-03.1	Mechanisms exist to communicate with users about their roles and responsibilities to maintain a safe and secure working environment.	8	
M1.2-POF3	Privacy awareness and training	The entity provides a privacy awareness program about its privacy policies and related matters, and provides specific training for selected personnel depending on their roles and responsibilities.	Functional	Intersects With	Formal Indoctrination	HRS-04.2	Mechanisms exist to formally educate authorized users on proper data handling practices for all the relevant types of data to which they have access.	8	
M1.2-POF3	Privacy awareness and training	The entity provides a privacy awareness program about its privacy policies and related matters, and provides specific training for selected personnel depending on their roles and responsibilities.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	8	
M1.2-POF3	Privacy awareness and training	The entity provides a privacy awareness program about its privacy policies and related matters, and provides specific training for selected personnel depending on their roles and responsibilities.	Functional	Intersects With	Sensitive / Regulated Data Storage, Handling & Processing	SAT-03.3	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive/regulated data is formally trained in data handling requirements.	8	
M1.2-POF4	Qualifications of internal personnel	The entity establishes qualifications for personnel responsible for protecting the privacy and security of PI and assigns such responsibilities only to those personnel who meet these qualifications and who have received training.	Functional	Intersects With	Competency Requirements for Security-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	8	EU GDPR Articles 37 (5); 38 (2)
M1.2-POF5	Policy changes	The entity has a process for evaluating and addressing the potential impacts of required changes to information privacy policy and procedures as changes occur in entity operations and operating locations, and as applicable jurisdictional laws and regulations are enacted to become new regulatory compliance requirements.	Functional	Subset Of	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	10	Article 6 (4)
M1.2-POF6	Oversight and monitoring	The entity has a process for governing and overseeing the application of policies and procedures.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	EU GDPR Articles 27 (1), (2), (3), (4), (5); 31; 38 (3), (5)
M1.2-POF6	Oversight and monitoring	The entity has a process for governing and overseeing the application of policies and procedures.	Functional	Intersects With	Non-Compliance Oversight	CPL-01.1	Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions.	8	EU GDPR Articles 27 (1), (2), (3), (4), (5); 31; 38 (3), (5)
M1.2-POF7	Policy compliance	The entity has procedures for identifying and addressing instances when non-compliance with information privacy policies and procedures are identified.	Functional	Intersects With	Non-Compliance Oversight	CPL-01.1	Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions.	8	
M1.2-POF8	Policy communications	The entity communicates its information privacy policies to internal personnel and other external third parties engaged in providing business process, IT services and information privacy support.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	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	Notes
M1.2-POF9	Consistency of commitments with privacy policies and procedures	The entity's internal personnel or advisers review contracts for consistency with privacy policies and procedures and address any inconsistencies.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	8	
M1.3	N/A	The entity has established policies and procedures for identifying, classifying and prioritizing the criticality of its collected PI. The entity also has procedures for evaluating potential vulnerabilities and the risk of unauthorized privacy information access, removal and destruction. The entity has designed and implemented control activities to help prevent, detect, address and notify relevant authorities in the event it detects and confirms instances of system and privacy information breaches. These policies and procedures were designed to help the entity meet its objectives related to privacy.	Functional	Intersects With	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	8	
M1.3	N/A	The entity has established policies and procedures for identifying, classifying and prioritizing the criticality of its collected PI. The entity also has procedures for evaluating potential vulnerabilities and the risk of unauthorized privacy information access, removal and destruction. The entity has designed and implemented control activities to help prevent, detect, address and notify relevant authorities in the event it detects and confirms instances of system and privacy information breaches. These policies and procedures were designed to help the entity meet its objectives related to privacy.	Functional	Intersects With	Personal Data (PD) Categories	PRI-05.7	Mechanisms exist to define and implement data handling and protection requirements for specific categories of sensitive Personal Data (PD).	8	
M1.3-POF1	Data and information classification	The entity has a process for classifying PI according to applicable regulation and risks associated with unauthorized disclosure or misuse.	Functional	Intersects With	Personal Data (PD) Categories	PRI-05.7	Mechanisms exist to define and implement data handling and protection requirements for specific categories of sensitive Personal Data (PD).	8	Article 30 (1), (2), (3), (4), (5)
M1.3-POF2	Privacy (risk) impact assessment	The entity performs a privacy (risk) impact assessment to identify and evaluate privacy specific risks, vulnerabilities and scenarios that could result in a system or information privacy breach situation. Privacy (risk) impact assessments are also used to identify security control weaknesses that need to be addressed as well as to report upon the entity's ability to comply with applicable system and privacy information breach notification laws and regulations.	Functional	Intersects With	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	8	EU GDPR Articles 35 (1), (2), (3), (4), (5), (7), (8), (10), (11); 36 (1), (2)
M1.3-POF3	Privacy incident response plan	The entity has a comprehensive privacy incident and breach management plan which provides examples of unauthorized uses and disclosures, as well as guidelines to determine whether an incident constitutes a breach. The plan is communicated to personnel who handle PI.	Functional	Subset Of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	10	EU GDPR Articles 5 (1) (f); 33 (1), (2), (3), (4), (5); 34 (1), (2), (3), (4)
M1.3-POF3	Privacy incident response plan	The entity has a comprehensive privacy incident and breach management plan which provides examples of unauthorized uses and disclosures, as well as guidelines to determine whether an incident constitutes a breach. The plan is communicated to personnel who handle PI.	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	8	EU GDPR Articles 5 (1) (f); 33 (1), (2), (3), (4), (5); 34 (1), (2), (3), (4)
M1.3-POF3	Privacy incident response plan	The entity has a comprehensive privacy incident and breach management plan which provides examples of unauthorized uses and disclosures, as well as guidelines to determine whether an incident constitutes a breach. The plan is communicated to personnel who handle PI.	Functional	Intersects With	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	8	EU GDPR Articles 5 (1) (f); 33 (1), (2), (3), (4), (5); 34 (1), (2), (3), (4)
M1.3-POF4	Ongoing and separate evaluations	The entity has a process for performing ongoing and separate evaluations of the design and operating effectiveness of information privacy and security controls and for addressing any identified control deficiencies.	Functional	Intersects With	Commitment To Continual Improvements	GOV-01.3	Mechanisms exist to commit appropriate resources needed for continual improvement of the organization's Security, Compliance & Resilience Program (SCRP), including: (1) Staffing; (2) Budget; (3) Processes; and (4) Technologies.	5	EU GDPR Articles 32 (3); 40 (1), (2), (3), (4)
M1.3-POF4	Ongoing and separate evaluations	The entity has a process for performing ongoing and separate evaluations of the design and operating effectiveness of information privacy and security controls and for addressing any identified control deficiencies.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	8	EU GDPR Articles 32 (3); 40 (1), (2), (3), (4)
M1.4	N/A	The entity has a process for identifying, locating and classifying its PI. This process is clearly described as an essential aspect of its data governance program which is aligned with its information security controls. Relevant control activity policies and procedures have been designed and placed into operation to achieve the entity's objectives related to privacy.	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	8	
M1.4	N/A	The entity has a process for identifying, locating and classifying its PI. This process is clearly described as an essential aspect of its data governance program which is aligned with its information security controls. Relevant control activity policies and procedures have been designed and placed into operation to achieve the entity's objectives related to privacy.	Functional	Intersects With	Sensitive Data Inventories	DCH-06.2	Mechanisms exist to maintain inventory logs of all sensitive media and conduct sensitive media inventories at least annually.	8	
M1.4	N/A	The entity has a process for identifying, locating and classifying its PI. This process is clearly described as an essential aspect of its data governance program which is aligned with its information security controls. Relevant control activity policies and procedures have been designed and placed into operation to achieve the entity's objectives related to privacy.	Functional	Intersects With	Inventory of Personal Data (PD)	PRI-05.5	Mechanisms exist to establish and maintain a current inventory of all Technology Assets, Applications and/or Services (TAAS) that collect, receive, process, store, transmit, share, update and/or dispose Personal Data (PD).	8	
M1.4-POF1	Data privacy security controls	The entity has a process to identify the specific or key data privacy security controls that it has designed and placed into operation that help reduce the risks of a data breach or a theft, erasure or alteration of PI.	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), (2)
N2.0	Agreement, notice and communication	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control EU GDPR Articles 12, 13, 14, 15, 18, 21
N2.1	N/A	The entity executes formal agreements, provides notices and formally communicates with data subjects about its privacy practices to meet its objectives related to privacy.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations; (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
N2.1-POF1	Agreements, notices and communications	The entity's agreements with data subjects formally capture data subject consents for sharing their PI with the entity and third parties affiliated with the entity, and for situations where the entity assembles, creates or purchases a data subject's PI, and when the entity needs to change the original purposes for obtaining a data subject's PI to meet the entity's changing business, operational or legal requirements.	Functional	Intersects With	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (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.	8	EU GDPR Articles 12 (1); 14 (1), (2), (3), (4), (5); 15 (1), (2); 18 (3)
N2.1-POF1	Agreements, notices and communications	The entity's agreements with data subjects formally capture data subject consents for sharing their PI with the entity and third parties affiliated with the entity, and for situations where the entity assembles, creates or purchases a data subject's PI, and when the entity needs to change the original purposes for obtaining a data subject's PI to meet the entity's changing business, operational or legal requirements.	Functional	Intersects With	Just-In-Time Notice & Updated Consent	PRI-03.2	Mechanisms exist to present data subjects with a new or updated consent request to collect, receive, process, store, transmit, share, update and/or dispose Personal Data (PD) in conjunction with the data action, when: (1) The original circumstances under which an individual gave consent have changed; or (2) A significant amount of time has passed since an individual gave consent.	5	EU GDPR Articles 12 (1); 14 (1), (2), (3), (4), (5); 15 (1), (2); 18 (3)
N2.1-POF2	Ongoing notices and communications	The entity has a process for periodically informing data subjects of its continued need for PI. The entity also has a process for obtaining the data subject's continued agreement and consent to use the data, and for informing data subjects when the entity suspects or learns, through ongoing monitoring and testing, that its systems (and systems of third parties providing services to the entity) have been breached and PI has been accessed, altered or removed in an unauthorized manner.	Functional	Intersects With	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations; (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	8	EU GDPR Articles 13 (2), (3); 21 (4)
N2.1-POF2	Ongoing notices and communications	The entity has a process for periodically informing data subjects of its continued need for PI. The entity also has a process for obtaining the data subject's continued agreement and consent to use the data, and for informing data subjects when the entity suspects or learns, through ongoing monitoring and testing, that its systems (and systems of third parties providing services to the entity) have been breached and PI has been accessed, altered or removed in an unauthorized manner.	Functional	Intersects With	Just-In-Time Notice & Updated Consent	PRI-03.2	Mechanisms exist to present data subjects with a new or updated consent request to collect, receive, process, store, transmit, share, update and/or dispose Personal Data (PD) in conjunction with the data action, when: (1) The original circumstances under which an individual gave consent have changed; or (2) A significant amount of time has passed since an individual gave consent.	8	EU GDPR Articles 13 (2), (3); 21 (4)
N2.1-POF3	Entities and activities covered	The entity has an objective description of the entities and activities covered by the privacy policies and procedures that is included in the entity's privacy notice.	Functional	Intersects With	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations; (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	8	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
N2.1-POF4	Clear and conspicuous	The entity's privacy notice is conspicuous and uses clear language.	Functional	Intersects With	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations; (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	8	
N2.1-POF5	Data subject revocations	When required, the entity has a process that provides data subjects a mechanism with which to request the entity to remove, dispose and erase a data subject's PI. Once a data subject's PI is no longer being stored in the entity's systems (this includes other affiliates and third parties that may also hold or store privacy information on behalf of the entity), the entity notifies the affected data subjects that such information has been removed.	Functional	Intersects With	Revoke Consent	PRI-03.4	Mechanisms exist to allow data subjects to revoke consent to collect, receive, process, store, transmit, share and/or update their Personal Data (PD).	8	
N2.2	N/A	Changes to privacy agreements are communicated in formal notices to affected data subjects. The updated agreements are re-executed by data subjects to reflect the changes made to the entity's privacy practices. Data subjects are also notified, and the agreements are updated in situations where the originally intended purposes for collecting a data subject's PI need to be updated or changed. Such notifications and communications are consistent with the entity's objectives related to privacy.	Functional	Intersects With	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations; (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	8	
N2.2	N/A	Changes to privacy agreements are communicated in formal notices to affected data subjects. The updated agreements are re-executed by data subjects to reflect the changes made to the entity's privacy practices. Data subjects are also notified, and the agreements are updated in situations where the originally intended purposes for collecting a data subject's PI need to be updated or changed. Such notifications and communications are consistent with the entity's objectives related to privacy.	Functional	Intersects With	Just-In-Time Notice & Updated Consent	PRI-03.2	Mechanisms exist to present data subjects with a new or updated consent request to collect, receive, process, store, transmit, share, update and/or dispose Personal Data (PD) in conjunction with the data action, when: (1) The original circumstances under which an individual gave consent have changed; or (2) A significant amount of time has passed since an individual gave consent.	8	
N2.2-POF1	Changes to privacy agreements/notices	The entity has policies and procedures it follows when it is determined that changes are needed to its privacy agreements/ notices. The entity documents the reasons for such changes and these changes are formally approved by an authorized member of management prior to being implemented. When required, the entity also notifies affected data subjects and obtains their formal approval (consent) prior to continuing to use or process a data subject's PI.	Functional	Intersects With	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.	5	
N2.2-POF1	Changes to privacy agreements/notices	The entity has policies and procedures it follows when it is determined that changes are needed to its privacy agreements/ notices. The entity documents the reasons for such changes and these changes are formally approved by an authorized member of management prior to being implemented. When required, the entity also notifies affected data subjects and obtains their formal approval (consent) prior to continuing to use or process a data subject's PI.	Functional	Intersects With	Chief Privacy Officer (CPO)	PRI-01.1	Mechanisms exist to appoints a Chief Privacy Officer (CPO) or similar role, with the authority, mission, accountability and resources to coordinate, develop and implement, applicable data privacy requirements and manage data privacy risks through the organization-wide data privacy program.	5	
N2.2-POF1	Changes to privacy agreements/notices	The entity has policies and procedures it follows when it is determined that changes are needed to its privacy agreements/ notices. The entity documents the reasons for such changes and these changes are formally approved by an authorized member of management prior to being implemented. When required, the entity also notifies affected data subjects and obtains their formal approval (consent) prior to continuing to use or process a data subject's PI.	Functional	Intersects With	Reasonable Data Privacy Practices	PRI-01.11	Mechanisms exist to limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of Personal Data (PD) according to reasonable consumer expectations for what is necessary and proportionate.	5	
C3.0	Collection and creation	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control EU GDPR Articles 5, 6, 7, 8, 9, 10, 11, 21, 25, 49
C3.1	N/A	The entity communicates available options regarding the collection and creation of PI and the consequences of each choice, including the data subject's option to reject their agreed consent for the entity to initially or subsequently collect and create PI.	Functional	Intersects With	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (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.	8	
C3.1-POF1	Communicates to data subjects	Data subjects are informed about the choices available to them with respect to the collection, use and disclosure of PI. Data subjects are informed that implicit or explicit consent is required to collect, use and disclose PI, unless a law or regulation specifically requires or allows otherwise.	Functional	Intersects With	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (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.	8	Article 8 (1), (2)
C3.1-POF2	Ability to opt-out	The entity has a process to allow data subjects with the option of not providing their PI, according to the data privacy agreement, including notifying the data subjects of the consequences of not agreeing to its provision and use by the entity	Functional	Intersects With	Notice of Right To Opt-Out	PRI-21	Mechanisms exist to include a notification to data subjects within the data privacy notice of: (1) Their right to direct an organization that sells or shares their Personal Data (PD) to stop selling or sharing their PD; and (2) The methods available to exercise that right.	8	
C3.1-POF2	Ability to opt-out	The entity has a process to allow data subjects with the option of not providing their PI, according to the data privacy agreement, including notifying the data subjects of the consequences of not agreeing to its provision and use by the entity	Functional	Intersects With	Product or Service Delivery Restrictions	PRI-03.5	Mechanisms exist to prevent discrimination against a data subject for exercising their legal rights pertaining to modifying or revoking consent, including prohibiting: (1) Refusing products and/or services; (2) Charging different rates for goods and/or services; and (3) Providing different levels of quality.	5	
C3.1-POF3	Communicates consequences of denying or withdrawing consent	When PI is collected, data subjects are informed of the consequences of refusing to provide PI for purposes identified in the notice.	Functional	Intersects With	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations; (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5	Article 21 (5)
C3.1-POF3	Communicates consequences of denying or withdrawing consent	When PI is collected, data subjects are informed of the consequences of refusing to provide PI for purposes identified in the notice.	Functional	Intersects With	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; (2) A means for users to decline the authorization; and (3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	5	Article 21 (5)
C3.1-POF3	Communicates consequences of denying or withdrawing consent	When PI is collected, data subjects are informed of the consequences of refusing to provide PI for purposes identified in the notice.	Functional	Intersects With	Product or Service Delivery Restrictions	PRI-03.5	Mechanisms exist to prevent discrimination against a data subject for exercising their legal rights pertaining to modifying or revoking consent, including prohibiting: (1) Refusing products and/or services; (2) Charging different rates for goods and/or services; and (3) Providing different levels of quality.	5	Article 21 (5)
C3.1-POF4	PI collection and creation	The entity has a process to collect and create (rendering and aggregating from multiple sources or information providers) PI as identified in the entity's privacy agreements. The process is consistent with its objectives related to privacy.	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.	8	EU GDPR Articles 5 (1)(b), (1)(c); 9 (2), (3); 10; 11 (1); 25 (2)
C3.2	N/A	The data subject's agreed consent is explicitly obtained and is only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent, when implicit consent is allowed as an available option, is documented.	Functional	Intersects With	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (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.	8	
C3.2-POF1	Documents and obtained consent for new purposes and uses	If information that was previously collected is to be used for purposes not previously identified in the privacy notice, the new purpose is documented, the data subject is notified, and implicit or explicit consent is obtained prior to such new use or purpose.	Functional	Intersects With	Purpose Specification	PRI-02.1	Mechanisms exist to ensure data privacy notices identify the purpose(s) for which Personal Data (PD) is collected, received, processed, stored, transmitted and/or shared.	8	Article 6 (4)
C3.2-POF1	Documents and obtained consent for new purposes and uses	If information that was previously collected is to be used for purposes not previously identified in the privacy notice, the new purpose is documented, the data subject is notified, and implicit or explicit consent is obtained prior to such new use or purpose.	Functional	Intersects With	Just-In-Time Notice & Updated Consent	PRI-03.2	Mechanisms exist to present data subjects with a new or updated consent request to collect, receive, process, store, transmit, share, update and/or dispose Personal Data (PD) in conjunction with the data action, when: (1) The original circumstances under which an individual gave consent have changed; or (2) A significant amount of time has passed since an individual gave consent.	8	Article 6 (4)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
C3.2-POF2	Explicit and implicit consent	The entity's policies and procedures require data subjects to explicitly agree and consent to the provision and collection of the data subject's PI. In some circumstances where the entity is unable to confirm explicit consent directly with a data subject, the entity's policies and procedures require the entity to formally document its rationale and basis for determining that it has obtained the data subject's implicit consent.	Functional	Intersects With	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; (2) A means for users to decline the authorization; and (3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	5	Article 7 (1), (2), (3), (4)
C3.2-POF2	Explicit and implicit consent	The entity's policies and procedures require data subjects to explicitly agree and consent to the provision and collection of the data subject's PI. In some circumstances where the entity is unable to confirm explicit consent directly with a data subject, the entity's policies and procedures require the entity to formally document its rationale and basis for determining that it has obtained the data subject's implicit consent.	Functional	Intersects With	Data Subject Opt-In Consent	PRI-03.12	Mechanisms exist to obtain consent from data subjects to opt-in for the following Personal Data (PD) actions: (1) Collecting; (2) Receiving; (3) Processing; (4) Storing; (5) Transmitting: (6) Sharing; and/or (7) Updating.	3	Article 7 (1), (2), (3), (4)
C3.2-POF3	Obtains explicit consent for sensitive information	Explicit consent is obtained directly from the data subject when sensitive PI is collected, used or disclosed, unless a law or regulation specifically requires otherwise.	Functional	Intersects With	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; (2) A means for users to decline the authorization; and (3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	5	EU GDPR Articles 7 (3); 49 (1), (2), (3)
C3.2-POF3	Obtains explicit consent for sensitive information	Explicit consent is obtained directly from the data subject when sensitive PI is collected, used or disclosed, unless a law or regulation specifically requires otherwise.	Functional	Intersects With	Data Subject Opt-In Consent	PRI-03.12	Mechanisms exist to obtain consent from data subjects to opt-in for the following Personal Data (PD) actions: (1) Collecting; (2) Receiving; (3) Processing; (4) Storing; (5) Transmitting: (6) Sharing; and/or (7) Updating.	3	EU GDPR Articles 7 (3); 49 (1), (2), (3)
C3.2-POF4	Obtains consent for data transfers	Consent is obtained before PI is transferred to or from an individual's computer or other similar device.	Functional	Intersects With	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (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.	8	
U4.0	Use, retention and disposal	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control EU GDPR Articles 5, 6, 7, 9, 10, 11, 15, 17, 18, 20, 21, 22, 25, 29, 32, 44, 45, 46, 49
U4.1	N/A	The entity limits the use of PI to the purposes identified in its objectives related to privacy	Functional	Intersects With	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to: (1) The purpose(s) originally collected, consistent with the data privacy notice(s); (2) What is authorized by the data subject, or authorized agent; and (3) What is consistent with applicable laws, regulations and contractual obligations.	8	
U4.1-POF1	Only uses PI for intended purposes	PI is used only for the intended purposes for which it was collected and only when implicit or explicit consent has been obtained unless a law or regulation specifically requires otherwise.	Functional	Intersects With	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to: (1) The purpose(s) originally collected, consistent with the data privacy notice(s); (2) What is authorized by the data subject, or authorized agent; and (3) What is consistent with applicable laws, regulations and contractual obligations.	8	EU GDPR Articles 5 (1)(a), (1)(b); 6 (1), (4); 7 (3); 9 (1), (2), (3); 10; 15 (4); 18 (1), (2); 20 (4); 21 (1), (2), (3), (6); 22 (1), (2), (3), (4); 25 (2); 29; 32 (4); 44; 45 (1); 46 (1), (2); 49 (1), (2), (3)
U4.2	N/A	The entity retains PI consistent with its objectives related to privacy.	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).	8	
U4.2-POF1	Retains PI	PI is retained for no longer than necessary to fulfill the stated purposes, unless a law or regulation specifically requires otherwise.	Functional	Subset Of	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	10	EU GDPR Articles 5 (1)(e); 11 (1); 17 (1)
U4.2-POF1	Retains PI	PI is retained for no longer than necessary to fulfill the stated purposes, unless a law or regulation specifically requires otherwise.	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).	8	EU GDPR Articles 5 (1)(e); 11 (1); 17 (1)
U4.2-POF2	Protects PI	Policies and procedures have been implemented to protect PI from erasure or destruction during the specified retention period of the information.	Functional	Subset Of	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	10	EU GDPR Articles 5 (1)(f); 25 (2); 46 (1), (2); 49 (1), (2), (3)
U4.3	N/A	The entity securely disposes of PI consistent with its objectives related to privacy.	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).	8	
U4.3-POF1	Captures, identifies and flags requests for deletion	Requests for deletion of PI are captured and information related to the requests is identified and flagged for destruction to meet the entity's objectives related to privacy.	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).	8	Article 17 (1), (2), (3)
U4.3-POF2	Disposes of, destroys and redacts PI	PI no longer retained is anonymized, disposed of or destroyed in a manner that prevents loss, theft, misuse or unauthorized access.	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).	8	
U4.3-POF3	Destroys PI	Policies and procedures are implemented to erase or otherwise destroy PI that has been identified for destruction.	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).	8	Article 25 (2)
A5.0	Access	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control EU GDPR Articles 11, 12, 15, 16, 20
A5.1	N/A	The entity grants identified and authenticated data subjects the ability to access their stored PI for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.	Functional	Intersects With	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	8	
A5.1-POF1	Authenticates data subjects' identities	The identity of data subjects who request access to their PI is authenticated before they are given access to that information.	Functional	Intersects With	Data Subject Authentication	PRI-06.8	Mechanisms exist to utilize reasonable consumer expectations to verify a data subject's identity, prior to taking action to disclose, share, correct, amend and/or delete Personal Data (PD).	8	EU GDPR Articles 11 (2), 12 (6)
A5.1-POF2	Permits data subjects access to their PI	Data subjects can determine whether the entity maintains PI about them and, upon request, may confirm and obtain access to their PI or request that the PI be returned, removed or erased.	Functional	Intersects With	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	8	EU GDPR Articles 15 (1), (3); 20 (1), (2), (3), (4)
A5.1-POF3	Provides understandable PI within reasonable time	PI is provided to data subjects in an understandable form, in a reasonable time frame and at a reasonable cost, if any.	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 12 (1), (3), (8)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
A5.1-POF4	Informs data subjects when access is denied	When data subjects are denied access to their PI, the entity informs them of the denial and the reasons for the denial in a timely manner, unless prohibited by law or regulation.	Functional	Intersects With	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	8	Article 12 (2), (4), (5)
A5.2	N/A	The entity corrects, amends or appends PI based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy.	Functional	Intersects With	Correcting Inaccurate Personal Data (PD)	PRI-06.1	Mechanisms exist to maintain a process for: (1) Data subjects to have inaccurate Personal Data (PD) maintained by the organization corrected or amended; and (2) Disseminating corrections or amendments of PD to other authorized users of the PD.	8	
A5.2-POF1	Communicates denial of access requests	Data subjects are informed, in writing, of the reason a request for access to their PI was denied, the source of the entity's legal right to deny such access, if applicable, and the individual's right, if any, to challenge such denial, as specifically permitted or required by law or regulation.	Functional	Intersects With	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	8	
A5.2-POF2	Permits data subjects to update or correct PI	Data subjects are able to update or correct PI held by the entity. The entity provides such updated or corrected information to third parties that were previously provided with the data subject's PI consistent with the entity's objective related to privacy.	Functional	Intersects With	Correcting Inaccurate Personal Data (PD)	PRI-06.1	Mechanisms exist to maintain a process for: (1) Data subjects to have inaccurate Personal Data (PD) maintained by the organization corrected or amended; and (2) Disseminating corrections or amendments of PD to other authorized users of the PD.	8	Article 16
A5.2-POF3	Communicates denial of correction requests	Data subjects are informed, in writing, about the reason a request for correction of PI was denied and how they may appeal.	Functional	Intersects With	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	8	
D6.0	Disclosure to third parties	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control EU GDPR Articles 12, 15, 19, 26, 28, 33, 34, 46, 47, 48, 49
D6.1	N/A	The entity discloses PI to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.	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.	8	
D6.1	N/A	The entity discloses PI to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.	Functional	Intersects With	Limiting Personal Data (PD) Disclosures	PRI-01.7	Mechanisms exist to limit the disclosure of Personal Data (PD) to authorized parties for the sole purpose for which the PD was obtained.	8	
D6.1-POF1	Communicates privacy policies to third parties	Privacy policies and specific instructions or requirements for handling PI are communicated to third parties to whom PI is disclosed.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
D6.1-POF1	Communicates privacy policies to third parties	Privacy policies and specific instructions or requirements for handling PI are communicated to third parties to whom PI is disclosed.	Functional	Intersects With	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.	8	
D6.1-POF2	Discloses PI only when appropriate	PI is disclosed to third parties only for the purposes for which it was collected or created and only when implicit or explicit consent has been obtained from the data subject, unless a law or regulation specifically requires otherwise	Functional	Intersects With	Limiting Personal Data (PD) Disclosures	PRI-01.7	Mechanisms exist to limit the disclosure of Personal Data (PD) to authorized parties for the sole purpose for which the PD was obtained.	8	EU GDPR Articles 19, 48
D6.1-POF3	Discloses PI only to appropriate third parties	PI is disclosed only to third parties who have agreements with the entity to protect PI in a manner consistent with the relevant aspects of the entity's privacy notice or other specific instructions or requirements. The entity has procedures in place to evaluate that the third parties have effective controls to meet the terms of the agreement, instructions or requirements.	Functional	Intersects With	Information Sharing With Third Parties	PRI-07	Mechanisms exist to disclose Personal Data (PD) to third-parties only for the purposes identified in the data privacy notice and with the implicit or explicit consent of the data subject.	8	
D6.1-POF4	Discloses information to third parties for new purposes and uses	PI is disclosed to third parties for new purposes or uses only with the prior implicit or explicit consent of data subjects	Functional	Intersects With	Information Sharing With Third Parties	PRI-07	Mechanisms exist to disclose Personal Data (PD) to third-parties only for the purposes identified in the data privacy notice and with the implicit or explicit consent of the data subject.	8	
D6.2	N/A	The entity creates and retains a complete, accurate and timely record of authorized disclosures of PI to meet the entity's objectives related to privacy.	Functional	Intersects With	Documenting Data Processing Activities	PRI-14	Mechanisms exist to document Personal Data (PD) processing activities that covers collection, receiving, processing, storage, transmission, sharing, updating and/or disposal actions with sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual requirements.	8	
D6.2	N/A	The entity creates and retains a complete, accurate and timely record of authorized disclosures of PI to meet the entity's objectives related to privacy.	Functional	Intersects With	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by: (1) The organization; and/or (2) Relevant third-parties that their PD was shared with.	8	
D6.2-POF1	Creates and retains record of authorized disclosures	The entity creates and maintains a record of authorized disclosures of PI that is complete, accurate and timely.	Functional	Intersects With	Documenting Data Processing Activities	PRI-14	Mechanisms exist to document Personal Data (PD) processing activities that covers collection, receiving, processing, storage, transmission, sharing, updating and/or disposal actions with sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual requirements.	8	Article 19
D6.2-POF1	Creates and retains record of authorized disclosures	The entity creates and maintains a record of authorized disclosures of PI that is complete, accurate and timely.	Functional	Intersects With	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by: (1) The organization; and/or (2) Relevant third-parties that their PD was shared with.	8	Article 19
D6.3	N/A	The entity creates and retains a complete, accurate and timely record of detected or reported unauthorized disclosures (including breaches) of PI to meet the entity's objectives related to privacy.	Functional	Intersects With	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by: (1) The organization; and/or (2) Relevant third-parties that their PD was shared with.	5	
D6.3-POF1	Creates and retains record of detected or reported unauthorized disclosures	The entity creates and maintains a record of detected or reported unauthorized disclosures of PI that is complete, accurate and timely.	Functional	Intersects With	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by: (1) The organization; and/or (2) Relevant third-parties that their PD was shared with.	5	Article 33 (5)
D6.4	N/A	The entity obtains privacy commitments from vendors and other third parties who have access to PI to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary	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.	8	
D6.4-POF1	Discloses PI only to appropriate third parties	PI is disclosed only to third parties who have agreements with the entity to protect PI in a manner consistent with the relevant aspects of the entity's privacy notice or other specific instructions or requirements. The entity has procedures in place to evaluate that the third parties have effective controls to meet the terms of the agreement, instructions or requirements.	Functional	Intersects With	Information Sharing With Third Parties	PRI-07	Mechanisms exist to disclose Personal Data (PD) to third-parties only for the purposes identified in the data privacy notice and with the implicit or explicit consent of the data subject.	8	EU GDPR Articles 26 (1), (2), (3); 28 (1), (2), (3), (4), (5), (6), (7), (8), (9); 46 (1), (2), (3); 47 (2); 49 (1), (2), (3)
D6.4-POF1	Discloses PI only to appropriate third parties	PI is disclosed only to third parties who have agreements with the entity to protect PI in a manner consistent with the relevant aspects of the entity's privacy notice or other specific instructions or requirements. The entity has procedures in place to evaluate that the third parties have effective controls to meet the terms of the agreement, instructions or requirements.	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5	EU GDPR Articles 26 (1), (2), (3); 28 (1), (2), (3), (4), (5), (6), (7), (8), (9); 46 (1), (2), (3); 47 (2); 49 (1), (2), (3)
D6.5	N/A	The entity obtains commitments from vendors and other third parties with access to PI to notify the entity in the event of actual or suspected unauthorized disclosures of PI. Such notifications are reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's objectives related to privacy.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	8	
D6.5-POF1	Remediates misuse of PI by third parties	The entity takes remedial action in response to misuse of PI by a third party to whom the entity has transferred such information	Functional	Intersects With	Break Clauses	TPM-05.7	Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for security, compliance and/or resilience controls.	3	
D6.5-POF1	Remediates misuse of PI by third parties	The entity takes remedial action in response to misuse of PI by a third party to whom the entity has transferred such information	Functional	Intersects With	Third-Party Deficiency Remediation	TPM-09	Mechanisms exist to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.	8	
D6.5-POF2	Reports actual or suspected unauthorized disclosures	A process exists for obtaining commitments from vendors and other third parties to report to the entity actual or suspected unauthorized disclosures of PI.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	8	Article 33 (2)
D6.5-POF2	Reports actual or suspected unauthorized disclosures	A process exists for obtaining commitments from vendors and other third parties to report to the entity actual or suspected unauthorized disclosures of PI.	Functional	Intersects With	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	8	Article 33 (2)
D6.6	N/A	The entity provides notification of breaches and incidents to affected data subjects, regulators and others to meet the entity's objectives related to privacy.	Functional	Intersects With	Data Breach	IRO-04.1	Mechanisms exist to address data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations.	8	
D6.6	N/A	The entity provides notification of breaches and incidents to affected data subjects, regulators and others to meet the entity's objectives related to privacy.	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.	8	
D6.6	N/A	The entity provides notification of breaches and incidents to affected data subjects, regulators and others to meet the entity's objectives related to privacy.	Functional	Intersects With	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	8	
D6.6-POF1	Remediates misuse of PI by third parties	The entity takes remedial action in response to misuse of PI by a third party to whom the entity has transferred such information	Functional	Intersects With	Break Clauses	TPM-05.7	Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for security, compliance and/or resilience controls.	3	
D6.6-POF1	Remediates misuse of PI by third parties	The entity takes remedial action in response to misuse of PI by a third party to whom the entity has transferred such information	Functional	Intersects With	Third-Party Deficiency Remediation	TPM-09	Mechanisms exist to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.	8	
D6.6-POF2	Provides notice of beaches and incidents	The entity has a process for providing notice of breaches and incidents to affected data subjects, regulators and others to meet the entity's objectives related to privacy.	Functional	Intersects With	Data Breach	IRO-04.1	Mechanisms exist to address data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations.	8	EU GDPR Articles 12 (1); 33 (1), (2), (3), (4); 34 (1), (2), (3), (4)
D6.6-POF2	Provides notice of beaches and incidents	The entity has a process for providing notice of breaches and incidents to affected data subjects, regulators and others to meet the entity's objectives related to privacy.	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.	8	EU GDPR Articles 12 (1); 33 (1), (2), (3), (4); 34 (1), (2), (3), (4)
D6.6-POF2	Provides notice of beaches and incidents	The entity has a process for providing notice of breaches and incidents to affected data subjects, regulators and others to meet the entity's objectives related to privacy.	Functional	Intersects With	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	8	EU GDPR Articles 12 (1); 33 (1), (2), (3), (4); 34 (1), (2), (3), (4)
D6.7	N/A	The entity provides data subjects with an accounting of the PI held and disclosure of the data subjects' PI, upon the data subjects' request, to meet the entity's objectives related to privacy.	Functional	Intersects With	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	8	
D6.7	N/A	The entity provides data subjects with an accounting of the PI held and disclosure of the data subjects' PI, upon the data subjects' request, to meet the entity's objectives related to privacy.	Functional	Intersects With	Personal Data (PD) Categories	PRI-05.7	Mechanisms exist to define and implement data handling and protection requirements for specific categories of sensitive Personal Data (PD).	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
D6.7	N/A	The entity provides data subjects with an accounting of the PI held and disclosure of the data subjects' PI, upon the data subjects' request, to meet the entity's objectives related to privacy.	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.	5	
D6.7-POF1	Identifies types of PI and handling processes	The types of PI and sensitive PI and the related processes, systems and third parties involved in the handling of such information are identified.	Functional	Intersects With	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	3	Article 15 (1)
D6.7-POF2	Captures, Identifies and Communicates Requests for Information	Requests for an accounting of PI held and disclosures of the data subjects' PI are captured, and information related to the requests is identified and communicated to data subjects to meet the entity's objectives related to privacy.	Functional	Intersects With	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	5	EU GDPR Articles 12 (1), (3); 19
S7.0	Security for privacy	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control EU GDPR Articles 5, 24, 25, 30, 32, 35, 45, 46
S7.1	N/A	The entity implements logical access security control software, infrastructures, authentication mechanisms and related architectures and security configuration controls over protected information assets to protect them from security incidents and events that might result in unauthorized access, alteration, destruction or disclosure of that information, and to meet the entity's privacy objectives.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
S7.1-POF1	Identifies and manages the inventory of information assets	The entity identifies, inventories, validates, classifies and manages information assets.	Functional	Subset Of	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10	Article 30 (1), (2), (3), (4), (5)
S7.1-POF2	Restricts logical and physical access to PI	The entity restricts logical and physical access to its information assets, including computing and network hardware, application systems, data (at-rest, during processing or in transmission), software, administrative authorities, mobile devices, output, and offline system components are restricted through the use of authentication and access control software and rule sets, and access to information assets is logged and monitored based on defined access authorizations.	Functional	Intersects With	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	8	EU GDPR Articles 25 (1); 32 (1)
S7.1-POF2	Restricts logical and physical access to PI	The entity restricts logical and physical access to its information assets, including computing and network hardware, application systems, data (at-rest, during processing or in transmission), software, administrative authorities, mobile devices, output, and offline system components are restricted through the use of authentication and access control software and rule sets, and access to information assets is logged and monitored based on defined access authorizations.	Functional	Intersects With	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	8	EU GDPR Articles 25 (1); 32 (1)
S7.1-POF2	Restricts logical and physical access to PI	The entity restricts logical and physical access to its information assets, including computing and network hardware, application systems, data (at-rest, during processing or in transmission), software, administrative authorities, mobile devices, output, and offline system components are restricted through the use of authentication and access control software and rule sets, and access to information assets is logged and monitored based on defined access authorizations.	Functional	Intersects With	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	8	EU GDPR Articles 25 (1); 32 (1)
S7.1-POF3	Identifies and authenticates users	Persons, infrastructure, network devices and software are identified and authenticated, and their access privileges are validated prior to granting access to information assets, whether locally or remotely.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	Article 32 (1)
S7.1-POF4	Considers network segmentation	The entity considers and, when deemed necessary, uses network segmentation to restrict access within and between its internal network segments and external networks. Segmentation permits unrelated portions of the entity's information system to be isolated from other network segments.	Functional	Intersects With	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate Technology Assets, Applications and/or Services (TAAS) to protect from other network resources.	8	Article 32 (1)
S7.1-POF5	Manages points of access	Points of access to the entity's information assets from internal and external users and outside entities and the types of data that flow through the points of access are identified, inventoried and managed. The types of users and the systems authorized to connect to each point of access are identified, authenticated and logged, and their activities within such systems are monitored.	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	Article 32 (1)
S7.1-POF6	Restricts access to information assets	The entity uses a combination of controls to restrict access to its information assets including data classification. The entity enforces logical separations of data structures and the segregation of incompatible duties applies device security hardening and security configuration policies, including activating system service restrictions, IP address validation and logical and physical access controls to servers and network device communication ports. The entity also uses updated access protocols to enable and enforce user and system access restrictions, user identification, authentication and logging, and user access behavior monitoring controls. The entity administrates digital certificate software tools to protect user communications and to enforce rules and policies for information asset access.	Functional	Intersects With	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	8	EU GDPR Articles 5 (1)(f), 32 (1)
S7.1-POF6	Restricts access to information assets	The entity uses a combination of controls to restrict access to its information assets including data classification. The entity enforces logical separations of data structures and the segregation of incompatible duties applies device security hardening and security configuration policies, including activating system service restrictions, IP address validation and logical and physical access controls to servers and network device communication ports. The entity also uses updated access protocols to enable and enforce user and system access restrictions, user identification, authentication and logging, and user access behavior monitoring controls. The entity administrates digital certificate software tools to protect user communications and to enforce rules and policies for information asset access.	Functional	Intersects With	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	8	EU GDPR Articles 5 (1)(f), 32 (1)
S7.1-POF7	Manages identification and authentication	User and system identification and authentication policy and procedure requirements are established, documented, managed, monitored and enforced for users and systems accessing the entity's information, infrastructure platforms and network devices, application systems, data storage systems and utility software.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	Article 32 (1)
S7.1-POF8	Manages credentials for infrastructure and software	The entity has established policies and procedures and technical specifications and requirements for the configuration and credentialing of users and systems prior to granting logical access to information and data about internally and externally managed infrastructure-based platforms, devices and software. The entity's procedures for provisioning and restricting access help make sure that systems and users are registered, authorized, documented and evaluated before access credentials and privileges are established and implemented via the network or from remote access points. User and system authorization and access credentials and privileges are removed and access is disabled when no longer required and when the infrastructure and software are no longer in use. The entity's procedures require that system and user access credentials be periodically revalidated for continued business need.	Functional	Intersects With	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	8	EU GDPR Articles 5 (1)(f), 32 (1)
S7.1-POF8	Manages credentials for infrastructure and software	The entity has established policies and procedures and technical specifications and requirements for the configuration and credentialing of users and systems prior to granting logical access to information and data about internally and externally managed infrastructure-based platforms, devices and software. The entity's procedures for provisioning and restricting access help make sure that systems and users are registered, authorized, documented and evaluated before access credentials and privileges are established and implemented via the network or from remote access points. User and system authorization and access credentials and privileges are removed and access is disabled when no longer required and when the infrastructure and software are no longer in use. The entity's procedures require that system and user access credentials be periodically revalidated for continued business need.	Functional	Intersects With	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	8	EU GDPR Articles 5 (1)(f), 32 (1)
S7.1-POF9	Uses encryption to protect data	The entity uses data encryption to supplement other measures to protect data in transit and at rest when such protections are deemed appropriate based on the assessed level of risk. The entity administrates, maintains and manages its encryption key management systems and regularly backs up its key stores to help these remain available in the event of a key management system outage or failure.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	Article 32 (1)(a)
S7.1-POF10	Protects encryption keys	Processes are in place to protect public and private encryption keys during generation, storage, use, deactivation and destruction.	Functional	Subset Of	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	10	Article 32 (1)(a)
S7.1-POF11	Uses antivirus and anti-malware software	The entity uses antivirus and anti-malware software and requires that it be implemented and maintained on all end-point devices connected to the internal and external networks to provide for the interception, detection and remediation of malware. The entity also requires third-party service organizations to confirm that their users and systems that connect to the entity's internal networks, infrastructure systems, network devices, application systems and data storage devices and information, also have active and currently updated antivirus and anti-malware protections.	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	8	Article 32 (1)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
S7.1-POF11	Uses antivirus and anti-malware software	The entity uses antivirus and anti-malware software and requires that it be implemented and maintained on all end-point devices connected to the internal and external networks to provide for the interception, detection and remediation of malware. The entity also requires third-party service organizations to confirm that their users and systems that connect to the entity's internal networks, infrastructure systems, network devices, application systems and data storage devices and information, also have active and currently updated antivirus and anti-malware protections.	Functional	Intersects With	Automatic Antimalware Signature Updates	END-04.1	Automated mechanisms exist to update antimalware technologies, including signature definitions.	8	Article 32 (1)
S7.2	N/A	The entity restricts physical access to facilities and protected information assets (e.g., data center facilities, back-up media storage and other sensitive locations) to authorized personnel to meet the entity's objectives.	Functional	Intersects With	Role-Based Physical Access	PES-02.1	Physical access control mechanisms exist to authorize physical access to facilities based on the position or role of the individual.	8	
S7.2	N/A	The entity restricts physical access to facilities and protected information assets (e.g., data center facilities, back-up media storage and other sensitive locations) to authorized personnel to meet the entity's objectives.	Functional	Intersects With	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	8	
S7.2-POF1	Managing physical access	The entity has implemented policies and procedures that restrict physical access to the entity's data centers, office spaces, documents, work areas and facilities based on an individual's needs for access, prior authorizations from a facility or system owner, and after the identity of each individual has been established prior to allowing access.	Functional	Intersects With	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	8	Article 5 (1)(f)
S7.2-POF2	Removes physical access	Processes are in place to remove physical access to facilities and system resources when an individual no longer requires access.	Functional	Intersects With	Removal of Assets	AST-11	Mechanisms exist to authorize, control and track technology assets entering and exiting organizational facilities.	8	
S7.2-POF3	Ongoing physical access monitoring	Processes are in place to periodically evaluate and re-validate (with the appropriate authorities) everyone's need for physical access and to make sure such access is consistent with the entity's business needs and the individual's specific job responsibilities.	Functional	Intersects With	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	8	
S7.2-POF3	Ongoing physical access monitoring	Processes are in place to periodically evaluate and re-validate (with the appropriate authorities) everyone's need for physical access and to make sure such access is consistent with the entity's business needs and the individual's specific job responsibilities.	Functional	Intersects With	Role-Based Physical Access	PES-02.1	Physical access control mechanisms exist to authorize physical access to facilities based on the position or role of the individual.	8	
S7.2-POF4	Internal physical access control	The entity requires individuals to be issued a proximity badge and has implemented proximity control mechanisms that require an individual to authenticate their identity via proximity card reading devices prior to gaining access to internal locations within the entity's data centers, office spaces, document storage locations, work areas and environmental control system locations	Functional	Intersects With	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	8	
S7.2-POF5	Physical protection of information on storage media	The entity has policies and procedures in place that address the physical protection of information and system and data storage devices and removable media. The policies and procedures include the handling and secure operation of such devices, and their removal from service, the removal of information assets residing on such devices and their eventual secured destruction.	Functional	Intersects With	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	8	
S7.2-POF5	Physical protection of information on storage media	The entity has policies and procedures in place that address the physical protection of information and system and data storage devices and removable media. The policies and procedures include the handling and secure operation of such devices, and their removal from service, the removal of information assets residing on such devices and their eventual secured destruction.	Functional	Intersects With	Lockable Physical Casings	PES-03.2	Physical access control mechanisms exist to protect system components from unauthorized physical access (e.g., lockable physical casings).	8	
S7.2-POF5	Physical protection of information on storage media	The entity has policies and procedures in place that address the physical protection of information and system and data storage devices and removable media. The policies and procedures include the handling and secure operation of such devices, and their removal from service, the removal of information assets residing on such devices and their eventual secured destruction.	Functional	Intersects With	Access To Critical Systems	PES-03.4	Physical access control mechanisms exist to enforce physical access to critical systems or sensitive/regulated data, in addition to the physical access controls for the facility.	8	
S7.2-POF5	Physical protection of information on storage media	The entity has policies and procedures in place that address the physical protection of information and system and data storage devices and removable media. The policies and procedures include the handling and secure operation of such devices, and their removal from service, the removal of information assets residing on such devices and their eventual secured destruction.	Functional	Intersects With	Physical Security of Offices, Rooms & Facilities	PES-04	Mechanisms exist to identify systems, equipment and respective operating environments that require limited physical access so that appropriate physical access controls are designed and implemented for offices, rooms and facilities.	8	
S7.2-POF6	Identifies environmental threats	As part of the risk assessment process, management identifies environmental threats that could impair the confidentiality, integrity and availability of systems, including threats resulting from adverse weather or the failure of physical access control and environmental control systems, or from electrical discharge, fire and water damage.	Functional	Intersects With	Supporting Utilities	PES-07	Facility security mechanisms exist to protect power equipment and power cabling for the system from damage and destruction.	8	Article 32 (1)(b)
S7.2-POF6	Identifies environmental threats	As part of the risk assessment process, management identifies environmental threats that could impair the confidentiality, integrity and availability of systems, including threats resulting from adverse weather or the failure of physical access control and environmental control systems, or from electrical discharge, fire and water damage.	Functional	Intersects With	Automatic Voltage Controls	PES-07.1	Facility security mechanisms exist to utilize automatic voltage controls for critical system components.	8	Article 32 (1)(b)
S7.2-POF6	Identifies environmental threats	As part of the risk assessment process, management identifies environmental threats that could impair the confidentiality, integrity and availability of systems, including threats resulting from adverse weather or the failure of physical access control and environmental control systems, or from electrical discharge, fire and water damage.	Functional	Intersects With	Emergency Shutoff	PES-07.2	Facility security mechanisms exist to shut off power in emergency situations by: (1) Placing emergency shutoff switches or devices in close proximity to systems or system components to facilitate safe and easy access for personnel; and (2) Protecting emergency power shutoff capability from unauthorized activation.	8	Article 32 (1)(b)
S7.2-POF6	Identifies environmental threats	As part of the risk assessment process, management identifies environmental threats that could impair the confidentiality, integrity and availability of systems, including threats resulting from adverse weather or the failure of physical access control and environmental control systems, or from electrical discharge, fire and water damage.	Functional	Intersects With	Emergency Power	PES-07.3	Facility security mechanisms exist to supply alternate power, capable of maintaining minimally-required operational capability, in the event of an extended loss of the primary power source.	8	Article 32 (1)(b)
S7.2-POF6	Identifies environmental threats	As part of the risk assessment process, management identifies environmental threats that could impair the confidentiality, integrity and availability of systems, including threats resulting from adverse weather or the failure of physical access control and environmental control systems, or from electrical discharge, fire and water damage.	Functional	Intersects With	Emergency Lighting	PES-07.4	Facility security mechanisms exist to utilize and maintain automatic emergency lighting that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.	8	Article 32 (1)(b)
S7.2-POF6	Identifies environmental threats	As part of the risk assessment process, management identifies environmental threats that could impair the confidentiality, integrity and availability of systems, including threats resulting from adverse weather or the failure of physical access control and environmental control systems, or from electrical discharge, fire and water damage.	Functional	Intersects With	Water Damage Protection	PES-07.5	Facility security mechanisms exist to protect systems from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly and known to key personnel.	8	Article 32 (1)(b)
S7.2-POF6	Identifies environmental threats	As part of the risk assessment process, management identifies environmental threats that could impair the confidentiality, integrity and availability of systems, including threats resulting from adverse weather or the failure of physical access control and environmental control systems, or from electrical discharge, fire and water damage.	Functional	Intersects With	Threat Catalog	THR-09	Mechanisms exist to develop and keep current a catalog of applicable internal and external threats to the organization, both natural and manmade.	8	Article 32 (1)(b)
S7.3	N/A	The entity restricts the transmission, movement and removal of information to authorized internal and external users and processes, and protects it during transmission, movement or removal to meet the entity's objectives.	Functional	Intersects With	Ad-Hoc Transfers	DCH-17	Mechanisms exist to secure ad-hoc exchanges of large digital files with internal or external parties.	5	
S7.3	N/A	The entity restricts the transmission, movement and removal of information to authorized internal and external users and processes, and protects it during transmission, movement or removal to meet the entity's objectives.	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	
S7.3	N/A	The entity restricts the transmission, movement and removal of information to authorized internal and external users and processes, and protects it during transmission, movement or removal to meet the entity's objectives.	Functional	Intersects With	Information Sharing With Third Parties	PRI-07	Mechanisms exist to disclose Personal Data (PD) to third-parties only for the purposes identified in the data privacy notice and with the implicit or explicit consent of the data subject.	8	
S7.3-POF1	Restricts the ability to perform transmission	Data loss prevention processes and technologies are used to restrict a user or system's ability to exfiltrate protected information, to execute data transmission, move information stored logically or maintained in physical devices, or otherwise modify, view, reproduce or destroy such information.	Functional	Intersects With	Data Loss Prevention (DLP)	NET-17	Automated mechanisms exist to implement Data Loss Prevention (DLP) to protect sensitive information as it is stored, transmitted and processed.	8	EU GDPR Articles 45 (1), 46 (1)
S7.3-POF2	Uses encryption technologies or secure communication channels to protect data	Encryption technologies or secure communication channels are used to protect data in transit and at rest, and communications of such data beyond the entity's established connectivity mechanisms are logical with physical access points.	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	8	Article 5 (1)(f)
S7.3-POF2	Uses encryption technologies or secure communication channels to protect data	Encryption technologies or secure communication channels are used to protect data in transit and at rest, and communications of such data beyond the entity's established connectivity mechanisms are logical with physical access points.	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	8	Article 5 (1)(f)
S7.3-POF3	Protects end point and mobile devices	Processes are in place to protect endpoint and mobile computing and personal productivity devices (such as laptop and desktop computers, servers, networking and data storage devices, smart phones and tablets) that are used in computing, networking, data storage and processing of the entity's information assets.	Functional	Intersects With	Endpoint Device Management (EDM)	END-01	Mechanisms exist to facilitate the implementation of Endpoint Device Management (EDM) controls.	8	
S7.3-POF3	Protects end point and mobile devices	Processes are in place to protect endpoint and mobile computing and personal productivity devices (such as laptop and desktop computers, servers, networking and data storage devices, smart phones and tablets) that are used in computing, networking, data storage and processing of the entity's information assets.	Functional	Intersects With	Unified Endpoint Device Management (UEDM)	END-01.1	Mechanisms exist to utilize a centralized Unified Endpoint Device Management (UEDM) solution that provides agent and/or agentless management of endpoint devices regardless of device location.	3	
S7.3-POF4	Protects removable media	Encryption technologies and physical (hardware) device protections are used for peripherals and remote data storage media (such as remote printers that store system-generated data, USB ports, drives, remote USB storage devices and data back-up media), as appropriate.	Functional	Intersects With	Removable Media Security	DCH-12	Mechanisms exist to restrict removable media in accordance with data handling and acceptable usage parameters.	8	
S7.4	N/A	The entity protects PI, in all forms, against accidental disclosure due to natural disasters and environmental hazards.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
S7.4	N/A	The entity protects PI, in all forms, against accidental disclosure due to natural disasters and environmental hazards.	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is processed and/or stored.	8	
S7.4-POF1	Continuity of physical and environmental protections	The entity has established policies and procedures that prevent, detect and react to system outages, incidents and events that disrupt system processing, or results in the loss, accidental disclosure or unauthorized modification of the entity's PI.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	Article 32 (2)
S7.5	N/A	The entity tests the effectiveness of the key administrative, technical and physical safeguards protecting personal data, periodically and as required by entity policy, or by relevant, applicable laws or regulations	Functional	Intersects With	Security, Compliance & Resilience Assessments	CPL-03	Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	8	
S7.5	N/A	The entity tests the effectiveness of the key administrative, technical and physical safeguards protecting personal data, periodically and as required by entity policy, or by relevant, applicable laws or regulations	Functional	Intersects With	Functional Review Of Security, Compliance & Resilience Controls	CPL-03.2	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's security, compliance and/or resilience policies and standards.	8	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
S7.5-POF1	Considers different types of ongoing and separate evaluations	Management uses a combination of different ongoing and separate evaluations, including system internal and external penetration testing, third-party independent verifications and certifications using established security control frameworks (NIST, COBIT, OWASP, etc.) and vendor and industry-specific, and the entity's own defined technical specifications, security requirements and configuration standards (e.g., performing ISO, PCI or TSP certifications), and internal audit assessments to monitor the effectiveness of required administrative, technical and physical safeguards.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	8	EU GDPR Articles 24 (1), (3); 25 (3); 32 (1)(d), (3); 35 (8)
S7.5-POF1	Considers different types of ongoing and separate evaluations	Management uses a combination of different ongoing and separate evaluations, including system internal and external penetration testing, third-party independent verifications and certifications using established security control frameworks (NIST, COBIT, OWASP, etc.) and vendor and industry-specific, and the entity's own defined technical specifications, security requirements and configuration standards (e.g., performing ISO, PCI or TSP certifications), and internal audit assessments to monitor the effectiveness of required administrative, technical and physical safeguards.	Functional	Intersects With	Security, Compliance & Resilience Assessments	CPL-03	Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	8	EU GDPR Articles 24 (1), (3); 25 (3); 32 (1)(d), (3); 35 (8)
S7.5-POF2	Implements incident management and recovery testing	Incident management and system recovery testing is performed on a periodic basis to make sure the entity continues to be able to identify, evaluate and respond to critical incidents. Testing includes: 1) the development and use of test scenarios based on the likelihood and magnitude of potential threats and known vulnerabilities; 2) consideration of system components that might impair system and information availability; 3) scenarios that consider the potential for key person availability; and 4) the updating of continuity and resiliency plans, procedures and systems based on test results.	Functional	Intersects With	Incident Response Testing	IRO-06	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	8	Article 32 (1)(c)
S7.5-POF3	Implements business continuity plan testing	The entity periodically tests the effectiveness of its business continuity and resiliency plans, procedures and capabilities to make sure that they continue to protect the entity from the adverse effects of unplanned system outages or damages that render systems and information assets unavailable or compromised. Testing includes: 1) the preparation and execution of risk scenario events that consider the likelihood and magnitude of identified threats and known vulnerabilities and system and process weaknesses; 2) the consideration of system components that could impair system processing and information confidentiality, integrity and availability; 3) scenarios that consider the potential impacts to key personnel availability; and 4) the update and revision of plans, processes and systems based on feedback and lessons learned from the results of testing.	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	8	Article 32 (1)(c)
S7.5-POF4	Testing confidentiality, completeness, integrity and availability of systems and back-up data	The continued confidentiality, completeness, integrity and availability of the entity's systems and back-up information is evaluated and confirmed on a periodic basis.	Functional	Intersects With	Testing for Reliability & Integrity	BCD-11.1	Mechanisms exist to routinely test backups that verify the reliability of the backup process, as well as the integrity and availability of the data.	8	Article 32 (1)(b)
S7.5-POF4	Testing confidentiality, completeness, integrity and availability of systems and back-up data	The continued confidentiality, completeness, integrity and availability of the entity's systems and back-up information is evaluated and confirmed on a periodic basis.	Functional	Intersects With	Test Restoration Using Sampling	BCD-11.5	Mechanisms exist to utilize sampling of available backups to test recovery capabilities as part of business continuity plan testing.	8	Article 32 (1)(b)
Q8.0	Data integrity and quality	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control Article 5
Q8.1	N/A	The entity collects and maintains accurate, reliable, up to date, complete and relevant PI to meet the entity's objectives related to privacy.	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.	8	
Q8.1-POF1	Communicates to data subjects	Individuals are informed that they are responsible for providing the entity with accurate and complete PI and for contacting the entity if correction of such information is required.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
Q8.1-POF2	Ensures accuracy and completeness of PI	PI is accurate and complete for the purposes for which it is to be used.	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.	8	Article 5 (1)(d)
Q8.1-POF3	Ensures relevance of PI	PI is relevant for the purposes for which it is to be used.	Functional	Intersects With	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to: (1) The purpose(s) originally collected, consistent with the data privacy notice(s); (2) What is authorized by the data subject, or authorized agent; and (3) What is consistent with applicable laws, regulations and contractual obligations.	8	
M9.0	Monitoring and enforcement	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control EU GDPR Articles 5, 22, 24, 25, 32, 35, 38
M9.1	N/A	The entity implements a process for receiving, addressing, resolving and communicating the resolution of inquiries, complaints and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner.	Functional	Intersects With	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	8	
M9.1-POF1	Communicates to data subjects	Data subjects are informed about how to contact the entity with inquiries, complaints and disputes.	Functional	Intersects With	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations; (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	8	Article 38 (4)
M9.1-POF2	Addresses inquiries, complaints and disputes	A process is in place to address inquiries, complaints and disputes.	Functional	Intersects With	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	8	Article 22 (3)
M9.1-POF3	Documents and communicates dispute resolution and recourse	Each complaint is addressed and the resolution is documented and communicated to the individual.	Functional	Intersects With	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	8	
M9.1-POF4	Documents and reports compliance review results	Compliance with objectives related to privacy are reviewed and documented and the results of such reviews are reported to management. If problems are identified, remediation plans are developed and implemented.	Functional	Intersects With	Non-Compliance Oversight	CPL-01.1	Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions.	8	
M9.1-POF5	Documents and reports instances of noncompliance	Instances of noncompliance with objectives related to privacy are documented and reported and, if needed, corrective and disciplinary measures are taken on a timely basis.	Functional	Intersects With	Non-Compliance Oversight	CPL-01.1	Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions.	8	
M9.1-POF6	Performs ongoing monitoring	Ongoing procedures are performed for monitoring the effectiveness of controls over PI and for taking timely corrective actions when necessary.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	8	