Annex 3 – Security Measures

Technical and organisational measures including technical and organisational measures to ensure the security of the data.

This annexure describes the adopted security measures cemented in an Information Security Management System (ISMS) for the purpose of protecting Personal Data and information, primarily with a view to meeting pre-defined requirements of applicable Data Protection Law and privacy law across Controller markets. These requirements have largely been derived from legislation across the Data Controller markets mandating fundamental security measures for the protection of Personal Data and are intended to provide a harmonised and single standard. We incorporate the requirements of data protection regulations into our control framework and reflect these requirements in policy and practice. Our data protection program which undergoes annual audits by third party auditors for conformity incorporates the following international standards: ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, and ISO/IEC 27701. These standards are integral to our approach to comply with global data protection regulations.

- ISO/IEC 27001: Provides a comprehensive framework for establishing, implementing, maintaining, and continually improving our ISMS, helping us manage the security of assets including financial information, intellectual property, employee details, and information entrusted to us by third parties.
- ISO/IEC 27017: Offers guidelines on the information security aspects specific to cloud computing, enhancing the existing controls in ISO/IEC 27001 by addressing cloud service-specific risks and controls.
- ISO/IEC 27018: A code of practice for protecting personal data in the cloud, ensuring that our cloud services adhere to applicable privacy regulations and best practices for personal data protection.
- ISO/IEC 27701: Extends ISO/IEC 27001 and ISO/IEC 27002 for privacy management within the company, helping us manage privacy risks related to personal information we process.

The control requirements in the table below are applied for the protection of Personal Data on behalf of the Data Controller, are fully implemented at Pexip, and are a subset of the controls within Pexip's data protection program.

Domain	Control	Control #	Control Description	Cybersecurity Framework	EMEA EU GDPR Mapping
Cybersecurity & Data Protection Governance	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	Govern	Art 32.1 Art 32.2 Art 32.3 Art 32.4
Cybersecurity & Data Protection Governance	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	Govern	Art 32.1 Art 32.2 Art 32.3 Art 32.4

Domain	Control	Control #	Control Description	Cybersecurity Framework	EMEA EU GDPR Mapping
Cybersecurity & Data Protection Governance	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & data privacy program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	Govern	Art 32.1 Art 32.2 Art 32.3 Art 32.4
Cybersecurity & Data Protection Governance	Contacts With Authorities	GOV-06	Mechanisms exist to identify and document appropriate contacts with relevant law enforcement and regulatory bodies.	Govern	Art 31 Art 36.1 Art 36.2 Art 36.3 Art 37.7 Art 40.1 Art 41.1 Art 42.2 Art 50
Cybersecurity & Data Protection Governance	Contacts With Groups & Associations	GOV-07	Mechanisms exist to establish contact with selected groups and associations within the cybersecurity & data privacy communities to: ▪ Facilitate ongoing cybersecurity & data privacy education and training for organizational personnel; ▪ Maintain currency with recommended cybersecurity & data privacy practices, techniques and technologies; and ▪ Share current cybersecurity and/or data privacy-related information including threats, vulnerabilities and incidents.	Govern	Art 40.2 Art 41.1 Art 42.2 Art 42.3 Art 43.2
Asset Management	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	Govern	Art 32.1 Art 32.2
Asset Management	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: ▪ Contain sufficient detail to assess the security of the network's architecture; ▪ Reflect the current architecture of the network environment; and ▪ Document all sensitive/regulated data flows.	Identify	Art 30.1 Art 30.2 Art 30.3 Art 30.4 Art 30.5
Business Continuity & Disaster Recovery	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	Govern	Art 32.1 Art 32.2
Capacity & Performance Planning	Capacity & Performance Management	CAP-01	Mechanisms exist to facilitate the implementation of capacity management controls to ensure optimal system performance to meet expected and anticipated future capacity requirements.	Govern	Art 32.1 Art 32.2
Change Management	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	Protect	Art 32.1 Art 32.2
Cloud Security	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	Govern	Art 32.1 Art 32.2

Domain	Control	Control #	Control Description	Cybersecurity Framework	EMEA EU GDPR Mapping
Compliance	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	Govern	Art 1.2 Art 2.1 Art 2.2 Art 3.1 Art 3.2 Art 3.3 Art 6.1 Art 17.3 Art 20.3 Art 23.1 Art 23.2 Art 24.1 Art 24.2 Art 24.3 Art 25.1 Art 25.2 Art 25.3 Art 27.1 Art 27.2 Art 27.3 Art 27.4 Art 27.5 Art 32.1 Art 32.2 Art 32.3 Art 32.4 Art 40.1 Art 40.2 Art 42.2 Art 43 Art 50
Compliance	Cybersecurity & Data Protection Controls Oversight	CPL-02	Mechanisms exist to provide a cybersecurity & data protection controls oversight function that reports to the organization's executive leadership.	Detect	Art 5.2
Compliance	Cybersecurity & Data Protection Assessments	CPL-03	Mechanisms exist to ensure managers regularly review the processes and documented procedures within their area of responsibility to adhere to appropriate cybersecurity & data protection policies, standards and other applicable requirements.	Detect	Art 5.2 Art 32.3
Compliance	Independent Assessors	CPL-03.1	Mechanisms exist to utilize independent assessors to evaluate cybersecurity & data protection controls at planned intervals or when the system, service or project undergoes significant changes.	Detect	Art 40.2 Art 42.1 Art 42.2 Art 42.3 Art 42.4 Art 42.6 Art 42.7 Art 43.2
Configuration Management	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	Govern	Art 32.1 Art 32.2
Continuous Monitoring	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	Govern	Art 32.1 Art 32.2

Domain	Control	Control #	Control Description	Cybersecurity Framework	EMEA EU GDPR Mapping
Cryptographic Protections	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	Govern	Art 5.1 Art 32.1 Art 32.2
Cryptographic Protections	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	Protect	Art 5.1
Cryptographic Protections	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	Protect	Art 5.1
Cryptographic Protections	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	Protect	Art 5.1
Data Classification & Handling	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	Govern	Art 5.1 Art 32.1 Art 32.2
Data Classification & Handling	Sanitization of Personal Data (PD)	DCH-09.3	Mechanisms exist to facilitate the sanitization of Personal Data (PD).	Protect	Art 5.1
Data Classification & Handling	Information Sharing	DCH-14	Mechanisms exist to utilize a process to assist users in making information sharing decisions to ensure data is appropriately protected.	Protect	Art 46
Data Classification & Handling	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	Protect	Art 5.1
Data Classification & Handling	Minimize Personal Data (PD)	DCH-18.1	Mechanisms exist to limit Personal Data (PD) being processed in the information lifecycle to elements identified in the Data Protection Impact Assessment (DPIA).	Protect	Art 35.1 Art 35.2 Art 35.3 Art 35.6 Art 35.8 Art 35.9 Art 35.11
Data Classification & Handling	Limit Personal Data (PD) Elements In Testing, Training & Research	DCH-18.2	Mechanisms exist to minimize the use of Personal Data (PD) for research, testing, or training, in accordance with the Data Protection Impact Assessment (DPIA).	Protect	Art 5.1 Art 35.1 Art 35.2 Art 35.3 Art 35.6 Art 35.8 Art 35.9 Art 35.11
Data Classification & Handling	Updating & Correcting Personal Data (PD)	DCH-22.1	Mechanisms exist to utilize technical controls to correct Personal Data (PD) that is inaccurate or outdated, incorrectly determined regarding impact, or incorrectly de-identified.	Protect	Art 12.3 Art 14.2 Art 16 Art 18.1 Art 26.3

Domain	Control	Control #	Control Description	Cybersecurity Framework	EMEA EU GDPR Mapping
Data Classification & Handling	Information Location	DCH-24	Mechanisms exist to identify and document the location of information and the specific system components on which the information resides.	Identify	Art 6.1 Art 26.1 Art 26.2 Art 27.3 Art 28.1 Art 28.2 Art 28.3 Art 28.4 Art 28.5 Art 28.6 Art 28.9 Art 28.10 Art 29 Art 44 Art 45.1 Art 45.2 Art 46.1 Art 46.2 Art 46.3 Art 47.1 Art 47.2 Art 48 Art 49.1 Art 49.2 Art 49.6
Data Classification & Handling	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.	Protect	Art 44 Art 45.1 Art 45.2 Art 46.1 Art 46.2 Art 46.3 Art 47.1 Art 47.2 Art 48 Art 49.1 Art 49.2 Art 49.6
Embedded Technology	Embedded Technology Security Program	EMB-01	Mechanisms exist to facilitate the implementation of embedded technology controls.	Protect	Art 32.1 Art 32.2
Endpoint Security	Endpoint Security	END-01	Mechanisms exist to facilitate the implementation of endpoint security controls.	Govern	Art 32.1 Art 32.2
Endpoint Security	Authorized Use	END-13.1	Mechanisms exist to utilize organization-defined measures so that data or information collected by sensors is only used for authorized purposes.	Protect	Art 5.2
Endpoint Security	Notice of Collection	END-13.2	Mechanisms exist to notify individuals that Personal Data (PD) is collected by sensors.	Identify	Art 5.1
Endpoint Security	Collection Minimization	END-13.3	Mechanisms exist to utilize sensors that are configured to minimize the collection of information about individuals.	Protect	Art 5.1
Human Resources Security	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	Govern	Art 32.1 Art 32.2 Art 32.4

Domain	Control	Control #	Control Description	Cybersecurity Framework	EMEA EU GDPR Mapping
Human Resources Security	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	Identify	Art 32.1 Art 32.2 Art 32.4
Identification & Authentication	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	Govern	Art 32.1 Art 32.2
Identification & Authentication	Pairwise Pseudonymous Identifiers (PPID)	IAC-09.6	Mechanisms exist to generate pairwise pseudonymous identifiers with no identifying information about a data subject to discourage activity tracking and profiling of the data subject.	Protect	Art 11.1
Incident Response	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity & data privacy-related incidents.	Govern	Art 32.1 Art 32.2
Incident Response	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.	Respond	Art 33.1 Art 33.2 Art 33.3 Art 33.4 Art 33.5
Incident Response	Integrated Security Incident Response Team (ISIRT)	IRO-07	Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity & data privacy incident response operations.	Respond	Art 34.1 Art 34.2 Art 34.3 Art 34.4
Incident Response	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: ▪ Internal stakeholders; ▪ Affected clients & third-parties; and ▪ Regulatory authorities.	Respond	Art 33.1 Art 33.2 Art 33.3 Art 33.4 Art 33.5 Art 34.1 Art 34.2 Art 34.3 Art 34.4
Incident Response	Coordination With External Providers	IRO-11.2	Mechanisms exist to establish a direct, cooperative relationship between the organization's incident response capability and external service providers.	Respond	Art 34.1 Art 34.2 Art 34.3 Art 34.4
Incident Response	Regulatory & Law Enforcement Contacts	IRO-14	Mechanisms exist to maintain incident response contacts with applicable regulatory and law enforcement agencies.	Identify	Art 31
Information Assurance	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of cybersecurity & data privacy assessment and authorization controls.	Govern	Art 32.1 Art 32.2 Art 32.3
Maintenance	Maintenance Operations	MNT-01	Mechanisms exist to develop, disseminate, review & update procedures to facilitate the implementation of maintenance controls across the enterprise.	Govern	Art 32.1 Art 32.2
Network Security	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	Govern	Art 32.1 Art 32.2
Physical & Environmental Security	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	Govern	Art 32.1 Art 32.2
Data Privacy	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data privacy controls.	Govern	Art 32.1 Art 32.2 Art 32.3 Art 32.4

Domain	Control	Control #	Control Description	Cybersecurity Framework	EMEA EU GDPR Mapping
Data Privacy	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.	Identify	Art 37.1 Art 38.1 Art 39.1 Art 39.2
Data Privacy	Data Protection Officer (DPO)	PRI-01.4	Mechanisms exist to appoint a Data Protection Officer (DPO): ▪ Based on the basis of professional qualities; and ▪ To be involved in all issues related to the protection of personal data.	Identify	Art 35.2 Art 37.1 Art 37.2 Art 37.3 Art 37.4 Art 37.5 Art 37.6 Art 37.7 Art 38.1 Art 38.2 Art 38.3 Art 38.4 Art 38.5 Art 38.6 Art 39.1 Art 39.2
Data Privacy	Data Privacy Notice	PRI-02	Mechanisms exist to: ▪ Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; ▪ Ensure that data privacy notices are clear and easy-to-understand, expressing information about Personal Data (PD) processing in plain language that meets all legal obligations; ▪ 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; ▪ Content of the privacy notice is periodically reviewed and updates made as necessary; and ▪ Retain prior versions of the privacy notice, in accordance with data retention requirements.	Identify	Art 11.2 Art 12.1 Art 13.1 Art 13.2 Art 13.3 Art 14.1 Art 14.2 Art 14.3 Art 26.1 Art 26.2
Data Privacy	Purpose Specification	PRI-02.1	Mechanisms exist to identify and document the purpose(s) for which Personal Data (PD) is collected, used, maintained and shared in its data privacy notices.	Identify	Art 13.1 Art 14.1 Art 14.2
Data Privacy	Automated Data Management Processes	PRI-02.2	Automated mechanisms exist to adjust data that is able to be collected, created, used, disseminated, maintained, retained and/or disclosed, based on updated data subject authorization(s).	Identify	Art 14.2 Art 22.1 Art 22.2 Art 22.3 Art 22.4
Data Privacy	Choice & Consent	PRI-03	Mechanisms exist to authorize the processing of their Personal Data (PD) prior to its collection that: ▪ Uses plain language and provide examples to illustrate the potential data privacy risks of the authorization; and ▪ Provides a means for users to decline the authorization.	Identify	Art 6.1 Art 7.1 Art 7.2 Art 7.3 Art 7.4 Art 8.1 Art 8.2 Art 12.6 Art 14.3

Domain	Control	Control #	Control Description	Cybersecurity Framework	EMEA EU GDPR Mapping
Data Privacy	Tailored Consent	PRI-03.1	Mechanisms exist to allow data subjects to modify the use permissions to selected attributes of their Personal Data (PD).	Identify	Art 7.1 Art 7.2 Art 7.3 Art 7.4 Art 12.2 Art 12.3 Art 12.4 Art 22.1 Art 22.2 Art 22.3 Art 22.4
Data Privacy	Just-In-Time Notice & Updated Consent	PRI-03.2	Mechanisms exist to present authorizations to process Personal Data (PD) in conjunction with the data action, when: ▪ The original circumstances under which an individual gave consent have changed; or ▪ A significant amount of time has passed since an individual gave consent.	Identify	Art 7.1 Art 7.2 Art 7.3 Art 7.4 Art 8.1 Art 8.2 Art 12.2 Art 12.3 Art 12.4 Art 13.3 Art 14.3 Art 21.4
Data Privacy	Restrict Collection To Identified Purpose	PRI-04	Mechanisms exist to collect Personal Data (PD) only for the purposes identified in the data privacy notice and includes protections against collecting PD from minors without appropriate parental, or legal guardian, consent.	Identify	Art 5.1
Data Privacy	Authority To Collect, Use, Maintain & Share Personal Data	PRI-04.1	Mechanisms exist to determine and document the legal authority that permits the collection, use, maintenance and sharing of Personal Data (PD), either generally or in support of a specific program or system need.	Identify	Art 5.1
Data Privacy	Personal Data Retention & Disposal	PRI-05	Mechanisms exist to: ▪ 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; ▪ Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage; and ▪ Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records).	Identify	Art 5.1 Art 18.1 Art 18.2 Art 21.1 Art 21.2 Art 21.3
Data Privacy	Internal Use of Personal Data For Testing, Training and Research	PRI-05.1	Mechanisms exist to address the use of Personal Data (PD) for internal testing, training and research that: ▪ Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes; and ▪ Authorizes the use of PD when such information is required for internal testing, training and research.	Identify	Art 5.1 Art 11.1 Art 18.1 Art 18.2
Data Privacy	Personal Data Accuracy & Integrity	PRI-05.2	Mechanisms exist to confirm the accuracy and relevance of Personal Data (PD) throughout the information lifecycle.	Identify	Art 5.1
Data Privacy	Data Masking	PRI-05.3	Mechanisms exist to mask sensitive/regulated data through data anonymization, pseudonymization, redaction or de-identification.	Identify	Art 5.1

Domain	Control	Control #	Control Description	Cybersecurity Framework	EMEA EU GDPR Mapping
Data Privacy	Usage Restrictions of Sensitive Personal Data	PRI-05.4	Mechanisms exist to restrict the use of Personal Data (PD) to only the authorized purpose(s) consistent with applicable laws, regulations and in data privacy notices.	Identify	Art 5.1 Art 9.1 Art 9.2 Art 10 Art 11.1 Art 18.1 Art 18.2
Data Privacy	Data Subject Access	PRI-06	Mechanisms exist to provide data subjects the ability to access their Personal Data (PD) maintained in organizational systems of records.	Identify	Art 12.1 Art 12.2 Art 13.2 Art 14.2 Art 15.1 Art 15.2 Art 15.3 Art 15.4 Art 16 Art 26.3
Data Privacy	Correcting Inaccurate Personal Data	PRI-06.1	Mechanisms exist to establish and implement a process for: ▪ Data subjects to have inaccurate Personal Data (PD) maintained by the organization corrected or amended; and ▪ Disseminating corrections or amendments of PD to other authorized users of the PD.	Respond	Art 12.3 Art 14.2 Art 16 Art 18.1 Art 26.3
Data Privacy	Notice of Correction or Processing Change	PRI-06.2	Mechanisms exist to notify affected data subjects if their Personal Data (PD) has been corrected or amended.	Respond	Art 12.3 Art 18.3 Art 19 Art 26.3
Data Privacy	Appeal Adverse Decision	PRI-06.3	Mechanisms exist to provide an organization-defined process for data subjects to appeal an adverse decision and have incorrect information amended.	Respond	Art 21.1 Art 21.2 Art 21.3 Art 26.3
Data Privacy	User Feedback Management	PRI-06.4	Mechanisms exist to implement a process for receiving and responding to complaints, concerns or questions from data subjects about the organizational data privacy practices.	Respond	Art 18.1 Art 18.2 Art 18.3 Art 19 Art 21.1 Art 21.6 Art 22 Art 26.3
Data Privacy	Right to Erasure	PRI-06.5	Mechanisms exist to erase Personal Data (PD) of a data subject without delay.	Respond	Art 17.1 Art 17.2 Art 17.3
Data Privacy	Data Portability	PRI-06.6	Mechanisms exist to export Personal Data (PD) in a structured, commonly used and machine-readable format that allows the data subject to transmit the data to another controller without hindrance.	Identify	Art 20.1 Art 20.2 Art 20.3 Art 20.4

Domain	Control	Control #	Control Description	Cybersecurity Framework	EMEA EU GDPR Mapping
Data Privacy	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.	Identify	Art 6.1 Art 6.4 Art 15.2 Art 20.2 Art 26.1 Art 26.2 Art 26.3 Art 44 Art 45.1 Art 45.2 Art 46.1 Art 46.2 Art 46.3 Art 47.1 Art 47.2 Art 48 Art 49.1 Art 49.2 Art 49.6
Data Privacy	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.	Identify	Art 6.1 Art 6.4 Art 26.1 Art 26.2 Art 26.3 Art 28.1 Art 28.2 Art 28.3 Art 28.4 Art 28.5 Art 28.6 Art 28.9 Art 28.10 Art 29
Data Privacy	Testing, Training & Monitoring	PRI-08	Mechanisms exist to conduct cybersecurity & data privacy testing, training and monitoring activities	Identify	Art 32.1 Art 32.2
Data Privacy	Personal Data Lineage	PRI-09	Mechanisms exist to utilize a record of processing activities to maintain a record of Personal Data (PD) that is stored, transmitted and/or processed under the organization's responsibility.	Identify	Art 30.1 Art 30.2 Art 30.3 Art 30.4 Art 30.5
Data Privacy	Data Quality Management	PRI-10	Mechanisms exist to manage the quality, utility, objectivity, integrity and impact determination and de-identification of sensitive/regulated data across the information lifecycle.	Identify	Art 5.1
Data Privacy	Automation	PRI-10.1	Automated mechanisms exist to support the evaluation of data quality across the information lifecycle.	Identify	Art 5.1 Art 21.5 Art 22
Data Privacy	Updating Personal Data (PD)	PRI-12	Mechanisms exist to develop processes to identify and record the method under which Personal Data (PD) is updated and the frequency that such updates occur.	Identify	Art 5.1

Domain	Control	Control #	Control Description	Cybersecurity Framework	EMEA EU GDPR Mapping
Data Privacy	Data Management Board	PRI-13	Mechanisms exist to establish a written charter for a Data Management Board (DMB) and assigned organization-defined roles to the DMB.	Identify	Art 5.1 Art 30.1 Art 30.2 Art 30.3 Art 30.4 Art 30.5
Data Privacy	Data Privacy Records & Reporting	PRI-14	Mechanisms exist to maintain data privacy-related records and develop, disseminate and update reports to internal senior management, as well as external oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory data privacy program mandates.	Identify	Art 31
Data Privacy	Accounting of Disclosures	PRI-14.1	Mechanisms exist to develop and maintain an accounting of disclosures of Personal Data (PD) held by the organization and make the accounting of disclosures available to the person named in the record, upon request.	Identify	Art 30.1 Art 30.2 Art 30.3 Art 30.4 Art 30.5
Data Privacy	Register As A Data Controller and/or Data Processor	PRI-15	Mechanisms exist to register as a data controller and/or data processor, including registering databases containing Personal Data (PD) with the appropriate Data Authority, when necessary.	Identify	Art 30.4
Project & Resource Management	Cybersecurity & Data Privacy Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of cybersecurity & data privacy-related resource planning controls that define a viable plan for achieving cybersecurity & data privacy objectives.	Govern	Art 32.1 Art 32.2
Risk Management	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	Govern	Art 32.1 Art 32.2
Risk Management	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's systems and data.	Identify	Art 35.1 Art 35.2 Art 35.3 Art 35.7 Art 35.8 Art 35.9 Art 35.11
Risk Management	Risk Register	RSK-04.1	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	Identify	Art 35.1
Risk Management	Business Impact Analysis (BIA)	RSK-08	Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess cybersecurity and data protection risks.	Identify	Art 35.1 Art 35.2 Art 35.3 Art 35.6 Art 35.8 Art 35.9 Art 35.11 Art 36.3
Risk Management	Supply Chain Risk Assessment	RSK-09.1	Mechanisms exist to periodically assess supply chain risks associated with systems, system components and services.	Identify	Art 35.1 Art 35.2 Art 35.3 Art 35.6 Art 35.8 Art 35.9 Art 35.11 Art 36.3

Domain	Control	Control #	Control Description	Cybersecurity Framework	EMEA EU GDPR Mapping
Risk Management	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	Identify	Art 35.1 Art 35.2 Art 35.3 Art 35.6 Art 35.8 Art 35.9 Art 35.11 Art 36.1 Art 36.2 Art 36.3
Secure Engineering & Architecture	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services.	Govern	Art 5.2 Art 24.1 Art 24.2 Art 24.3 Art 25.1 Art 25.2 Art 25.3 Art 32.1 Art 32.2 Art 40.2
Secure Engineering & Architecture	Centralized Management of Cybersecurity & Data Privacy Controls	SEA-01.1	Mechanisms exist to centrally-manage the organization-wide management and implementation of cybersecurity & data privacy controls and related processes.	Protect	Art 5.2 Art 24.1 Art 24.2 Art 24.3 Art 25.1 Art 25.2 Art 25.3 Art 32.1 Art 32.2 Art 40.2
Secure Engineering & Architecture	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for cybersecurity & data privacy principles that addresses risk to organizational operations, assets, individuals, other organizations.	Protect	Art 5.2 Art 24.1 Art 24.2 Art 24.3 Art 25.1 Art 25.2 Art 25.3 Art 32.1 Art 32.2 Art 40.2

Domain	Control	Control #	Control Description	Cybersecurity Framework	EMEA EU GDPR Mapping
Secure Engineering & Architecture	Standardized Terminology	SEA-02.1	Mechanisms exist to standardize technology and process terminology to reduce confusion amongst groups and departments.	Protect	Art 4.1 Art 4.2 Art 4.3 Art 4.4 Art 4.5 Art 4.6 Art 4.7 Art 4.8 Art 4.9 Art 4.10 Art 4.11 Art 4.12 Art 4.13 Art 4.14 Art 4.15 Art 4.16 Art 4.17 Art 4.18 Art 4.19 Art 4.20 Art 4.21 Art 4.22 Art 4.23 Art 4.24 Art 4.25 Art 4.26
Secure Engineering & Architecture	Defense-In-Depth (DiD) Architecture	SEA-03	Mechanisms exist to implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.	Protect	Art 5.2 Art 24.1 Art 24.2 Art 24.3 Art 25.1 Art 25.2 Art 25.3 Art 32.1 Art 32.2 Art 40.2

Domain	Control	Control #	Control Description	Cybersecurity Framework	EMEA EU GDPR Mapping
Secure Engineering & Architecture	Distributed Processing & Storage	SEA-15	Mechanisms exist to distribute processing and storage across multiple physical locations.	Protect	Art 6.1 Art 26.1 Art 26.2 Art 26.3 Art 28.1 Art 28.2 Art 28.3 Art 28.4 Art 28.5 Art 28.6 Art 28.9 Art 28.10 Art 29 Art 44 Art 45.1 Art 45.2 Art 46.1 Art 46.2 Art 46.3 Art 47.1 Art 47.2 Art 48 Art 49.1 Art 49.2 Art 49.6
Security Operations	Operations Security	OPS-01	Mechanisms exist to facilitate the implementation of operational security controls.	Govern	Art 32.1 Art 32.2
Security Awareness & Training	Cybersecurity & Data Privacy-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	Govern	Art 32.1 Art 32.2 Art 32.4
Technology Development & Acquisition	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	Govern	Art 32.1 Art 32.2
Third-Party Management	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	Govern	Art 28.1 Art 28.2 Art 28.3 Art 28.4 Art 28.5 Art 28.6 Art 28.9 Art 28.10 Art 32.1 Art 32.2
Third-Party Management	Supply Chain Protection	TPM-03	Mechanisms exist to evaluate security risks associated with the services and product supply chain.	Identify	Art 28.1 Art 28.2 Art 28.3 Art 28.4 Art 28.5 Art 28.6 Art 28.9 Art 28.10

Domain	Control	Control #	Control Description	Cybersecurity Framework	EMEA EU GDPR Mapping
Third-Party Management	Third-Party Processing, Storage and Service Locations	TPM-04.4	Mechanisms exist to restrict the location of information processing/storage based on business requirements.	Identify	Art 6.1 Art 6.4 Art 26.1 Art 26.2 Art 26.3 Art 28.1 Art 28.2 Art 28.3 Art 28.4 Art 28.5 Art 28.6 Art 28.9 Art 28.10 Art 29 Art 44 Art 45.1 Art 45.2 Art 46.1 Art 46.2 Art 46.3 Art 47.1 Art 47.2 Art 48 Art 49.1 Art 49.2 Art 49.6
Third-Party Management	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	Identify	Art 28.1 Art 28.2 Art 28.3 Art 28.4 Art 28.5 Art 28.6 Art 28.9 Art 28.10 Art 29
Threat Management	Threat Intelligence Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	Govern	Art 32.1 Art 32.2
Vulnerability & Patch Management	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	Govern	Art 32.1 Art 32.2
Vulnerability & Patch Management	Flaw Remediation with Personal Data (PD)	VPM-04.2	Mechanisms exist to identify and correct flaws related to the collection, usage, processing or dissemination of Personal Data (PD).	Identify	Art 5.1
Web Security	Web Security	WEB-01	Mechanisms exist to facilitate the implementation of an enterprise-wide web management policy, as well as associated standards, controls and procedures.	Govern	Art 32.1 Art 32.2
Web Security	Use of Demilitarized Zones (DMZ)	WEB-02	Mechanisms exist to utilize a Demilitarized Zone (DMZ) to restrict inbound traffic to authorized devices on certain services, protocols and ports.	Protect	Art 32.1 Art 32.2