Public Version - Annex 2 - Statement of Applicability for Pipedrive ISMS and PIMS (ISO27001:2022 / ISO27701:2019)

This document provides the control and justification for its inclusion and exclusion from the Pipedrive ISMS and PIMS

ISO 27001:2022 Annex A / ISO 27701:2019			
Ref	**Control**	**Control description**	**Implemented**
Section: 5 Organizational Controls			
ISMS A.5.1 PIMS 6.2.1.1 PIMS 6.2.1.2	Policies for information security and privacy	Information security and privacy policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.	yes

ISMS A.5.2 PIMS 6.3.1.1	Information security and privacy roles and responsibilities	Information security and privacy roles and responsibilities shall be defined and allocated according to the organization needs	yes
ISMS A.5.3 PIMS 6.3.1.2	Segregation of duties	Conflicting duties and conflicting areas of responsibility shall be segregated.	yes
ISMS 5.4 PIMS 6.4.2.1	Management responsibilities	Management shall require all personnel to apply information security and privacy in accordance with the established information security and privacy policy, topic-specific policies and procedures of the organization.	yes
ISMS A.5.5 PIMS 6.3.1.3	Contact with authorities	The organization shall establish and maintain contact with relevant authorities.	yes
ISMS A.5.6	Contact with special interest	The organization shall establish and maintain contact	yes

PIMS 6.3.1.4	groups	with special interest groups or other specialist security and privacy forums and professional associations.	
ISMS A.5.7	Threat intelligence	Information relating to information security and privacy threats shall be collected and analysed to produce threat intelligence.	yes
ISMS A.5.8 PIMS 6.3.1.5 PIMS 6.11.1.1	Information Security and Privacy in Project Management	Information security and privacy shall be integrated into project management.	yes
ISMS A.5.9 PIMS 6.5.1.1 PIMS 6.5.1.2	Inventory of information and other associated assets	An inventory of information and other associated assets, including owners, shall be developed and maintained.	yes

ISMS A.5.10 PIMS 6.5.1.3 PIMS 6.5.2.3	Acceptable use of information and other associated assets	Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented.	yes
ISMS A.5.11 PIMS 6.5.1.4	Return of assets	Personnel and other interested parties as appropriate shall return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.	yes
ISMS A.5.12 PIMS 6.5.2.1	Classification of information	Information shall be classified according to the information security and privacy needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.	yes
ISMS A.5.13	Labelling of information	An appropriate set of procedures for information labelling shall be developed	yes

PIMS 6.5.2.2		and implemented in accordance with the information classification scheme adopted by the organization.	
ISMS A.5.14 PIMS 6.10.2.1 PIMS 6.10.2.2 PIMS 6.10.2.3	Information transfer	Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organization and between the organization and other parties.	yes
ISMS A.5.15 PIMS 6.6.1.1 PIMS 6.6.1.2	Access control	Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security and privacy requirements.	yes
ISMS A.5.16	Identity management	The full life cycle of identities shall be managed.	yes

PIMS 6.6.2.1			
ISMS A.5.17 PIMS 6.6.2.4 PIMS 6.6.3.1 PIMS 6.6.4.3	Authentication information	Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information.	yes
ISMS A.5.18 PIMS 6.6.2.2 PIMS 6.6.2.5 PIMS 6.6.2.6	Access rights	Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.	yes
ISMS A.5.19 PIMS 6.12.1.1	Information security and privacy in supplier relationships	Processes and procedures shall be defined and implemented to manage the information security and	yes

		privacy risks associated with the use of supplier's products or services.	
ISMS A.5.20 PIMS 6.12.1.2	Addressing information security and privacy within supplier agreements	Relevant information security and privacy requirements shall be established and agreed with each supplier based on the type of supplier relationship.	yes
ISMS A.5.21 PIMS 6.12.1.3	Managing information security and privacy in the information and communication technology (ICT) supply chain	Processes and procedures shall be defined and implemented to manage the information security and privacy risks associated with the ICT products and services supply chain.	yes
ISMS A.5.22 PIMS 6.12.2.1 PIMS 6.12.2.2	Monitoring, review and change management of supplier services	The organization shall regularly monitor, review, evaluate and manage change in supplier information security and privacy practices and service delivery.	yes

ISMS A.5.23	Information security and privacy for use of cloud services	Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization's information security and privacy requirements.	yes
ISMS A.5.24 PIMS 6.13.1.1 PIMS 6.13.1.2	Information security and privacy incident management planning and preparation	The organization shall plan and prepare for managing information security and privacy incidents by defining, establishing and communicating information security and privacy incident management processes, roles and responsibilities.	yes
ISMS A.5.25 PIMS 6.13.1.4	Assessment and decision on information security and privacy events	The organization shall assess information security events and decide if they are to be categorized as information security and privacy incidents.	yes
ISMS A.5.26	Response to information	Information security and privacy incidents shall be responded to in accordance	yes

PIMS 6.13.1.5	security and privacy incidents	with the documented procedures.	
ISMS A.5.27 PIMS 6.13.1.6	Learning from Information security and privacy incidents	Knowledge gained from information security and privacy incidents shall be used to strengthen and improve the information security and privacy controls.	yes
ISMS A.5.28 PIMS 6.13.1.7	Collection of evidence	The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security and privacy events.	yes
ISMS A.5.29 PIMS 6.14.1.1 PIMS 6.14.1.2 PIMS 6.14.1.3	Information security and privacy during disruption	The organization shall plan how to maintain information security and privacy at an appropriate level during disruption.	yes

ISMS A.5.30	ICT readiness for business continuity	ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.	yes
ISMS A.5.31 PIMS 6.15.1.1 PIMS 6.15.1.5	Legal, statutory, regulatory and contractual requirements.	Legal, statutory, regulatory and contractual requirements relevant to information security and privacy and the organization's approach to meet these requirements shall be identified, documented and kept up to date.	yes
ISMS A.5.32 PIMS 6.15.1.2	Intellectual Property Rights	The organization shall implement appropriate procedures to protect intellectual property rights.	yes
ISMS A.5.33 PIMS 6.15.1.3	Protection of records	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release.	yes

ISMS A.5.34 PIMS 6.15.1.4	Privacy and protection of personally identifiable information (PII)	The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.	yes
ISMS A.5.35 PIMS 6.15.2.1	Independent review of information security and privacy	The organization’s approach to managing information security and privacy and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant changes occur.	yes
ISMS A.5.36 PIMS 6.15.2.2	Compliance with policies, rules and standards for information security and privacy	Compliance with the organization’s information security and privacy policy, topic-specific policies, rules and standards shall be regularly reviewed.	yes

ISMS A.5.37 PIMS 6.9.1.1	Documented operating procedures	Operating procedures for information processing facilities shall be documented and made available to personnel who need them.	yes
Section: 6 People controls			
ISMS A.6.1 PIMS 6.4.1.1	Screening	Background verification checks on all candidates to become personnel shall be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	yes
ISMS A.6.2 PIMS 6.4.1.2	Terms and conditions of employment	The employment contractual agreements shall state the personnel's and the organization's responsibilities	yes

		for information security and privacy.	
ISMS A.6.3 PIMS 6.4.2.2	Information security and privacy awareness, education and training	Personnel of the organization and relevant interested parties shall receive appropriate information security and privacy awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function.	yes
ISMS A.6.4 PIMS 6.4.2.3	Disciplinary process	A disciplinary process shall be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security and privacy policy violation.	yes
ISMS A.6.5	Responsibilities after termination	Information security and privacy responsibilities and duties that remain valid after	yes

PIMS 6.4.3.1	or change of employment	termination or change of employment shall be defined, enforced and communicated to relevant personnel and other interested parties.	
ISMS A.6.6 PIMS 6.10.2.4	Confidentiality or non-disclosure-agreements	Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.	yes
ISMS A.6.7 PIMS 6.3.2.2	Remote working	Security and privacy measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.	yes
ISMS A.6.8	Information security and	The organization shall provide a mechanism for personnel to report observed or suspected	yes

PIMS 6.13.1.2 PIMS 6.13.1.3	privacy event reporting	information security and privacy events through appropriate channels in a timely manner.	
Section: 7 Physical controls			
ISMS A.7.1 PIMS 6.8.1.1	Physical Security Perimeters	Security perimeters shall be defined and used to protect areas that contain information and other associated assets.	yes
ISMS A.7.2 PIMS 6.8.1.2 PIMS 6.8.1.6	Physical entry	Secure areas shall be protected by appropriate entry controls and access points.	yes
ISMS A.7.3 PIMS 6.8.1.3	Securing offices, rooms and facilities	Physical security for offices, rooms and facilities shall be designed and implemented.	yes

ISMS A.7.4	Physical security monitoring	Premises shall be continuously monitored for unauthorized physical access.	yes
ISMS A.7.5 PIMS 6.8.1.4	Protecting against physical and environmental threats	Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented.	yes
ISMS A.7.6 PIMS 6.8.1.5	Working in secure areas	Security measures for working in secure areas shall be designed and implemented.	yes
ISMS A.7.7 PIMS 6.8.2.9	Clear Desk and Clear Screen	Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced.	yes
ISMS A.7.8	Equipment siting and protection	Equipment shall be sited securely and protected.	yes

PIMS 6.8.2.1			
ISMS A.7.9 PIMS 6.8.2.6	Security of assets off-premises	Off-site assets shall be protected.	yes
ISMS A.7.10 PIMS 6.5.3.1 PIMS 6.5.3.2 PIMS 6.5.3.3 PIMS 6.8.2.5	Storage media	Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization’s classification scheme and handling requirements.	yes
ISMS A.7.11 PIMS 6.8.2.2	Supporting utilities	Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.	yes

ISMS A.7.12 PIMS 6.8.2.3	Cabling Security	Cables carrying power, data or supporting information services shall be protected from interception, interference or damage.	yes
ISMS A.7.13 PIMS 6.8.2.4	Equipment maintenance	Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information.	yes
ISMS A.7.14 PIMS 6.8.2.7	Secure disposal or reuse of equipment	Items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	yes
Section: 8 Technological controls			
ISMS A.8.1 PIMS 6.3.2.1	User end point devices	Information stored on, processed by or accessible via user end point devices shall be protected.	yes

PIMS 6.8.2.8			
ISMS A.8.2 PIMS 6.6.2.3	Privileged access rights	The allocation and use of privileged access rights shall be restricted and managed.	yes
ISMS A.8.3 PIMS 6.6.4.1	Information Access restriction	Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control.	yes
ISMS A.8.4 PIMS 6.6.4.5	Access to source code	Read and write access to source code, development tools and software libraries shall be appropriately managed.	yes
ISMS A.8.5 PIMS 6.6.4.2	Secure authentication	Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control.	yes

ISMS A.8.6 PIMS 6.9.1.3	Capacity Management	The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.	yes
ISMS A.8.7 PIMS 6.9.2.1	Protection against malware	Protection against malware shall be implemented and supported by appropriate user awareness.	yes
ISMS A.8.8 PIMS 6.9.6.1 PIMS 6.15.2.3	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems in use shall be obtained, the organization's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken.	yes
ISMS A.8.9	Configuration management	Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed.	yes

ISMS A.8.10	Information Deletion	Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.	yes
ISMS A.8.11	Data Masking	Data masking shall be used in accordance with the organization’s topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.	yes
ISMS A.8.12	Data leakage prevention	Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information.	yes

ISMS A.8.13 PIMS 6.9.3.1	Information backup	Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.	yes
ISMS A.8.14 PIMS 6.14.2.1	Redundancy of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	yes
ISMS A.8.15 PIMS 6.9.4.1 PIMS 6.9.4.2 PIMS 6.9.4.3	Logging	Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed.	yes
ISMS A.8.16	Monitoring activities	Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to	Yes

		evaluate potential information security and privacy incidents.	
ISMS A.8.17 PIMS 6.9.4.4	Clock synchronization	The clocks of information processing systems used by the organization shall be synchronized to approved time sources.	yes
ISMS A.8.18 PIMS 6.6.4.4	Use of privileged utility programs	The use of utility programs that can be capable of overriding system and application controls shall be restricted and tightly controlled.	yes
ISMS A.8.19 PIMS 6.9.5.1 PIMS 6.9.6.2	Installation of software on operational systems	Procedures and measures shall be implemented to securely manage software installation on operational systems.	yes
ISMS A.8.20 PIMS 6.10.1.1	Network Controls	Networks and network devices shall be secured, managed and controlled to protect information in systems and applications.	yes

ISMS A.8.21 PIMS 6.10.1.2	Security of network services	Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored.	yes
ISMS A.8.22 PIMS 6.10.1.3	Segregation ~~in~~ of networks	Groups of information services, users and information systems shall be segregated in the organization's networks.	yes
ISMS A.8.23	Web filtering	Access to external websites shall be managed to reduce exposure to malicious content.	yes
ISMS A.8.24 PIMS 6.7.1.1 PIMS 6.7.1.2	Use of cryptography	Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented.	yes
ISMS A.8.25	Secure development life cycle	Rules for the secure development of software and	yes

PIMS 6.11.2.1		systems shall be established and applied.	
ISMS A.8.26 PIMS 6.11.1.2 PIMS 6.11.1.3	Application security requirements	Information security requirements shall be identified, specified and approved when developing or acquiring applications.	yes
ISMS A.8.27 PIMS 6.11.2.5	Secure system architecture and engineering principles	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development activities.	yes
ISMS A.8.28	Secure coding	Secure coding principles shall be applied to software development.	yes
ISMS A.8.29 PIMS 6.11.2.8	Security testing in development and acceptance	Security testing processes shall be defined and implemented in the development life cycle.	yes

PIMS 6.11.2.9			
ISMS A.8.30 PIMS 6.11.2.7	Outsourced development	The organization shall direct, monitor and review the activities related to outsourced system development.	yes
ISMS A.8.31 PIMS 6.9.1.4 PIMS 6.11.2.6	Separation of development, test and production environments	Development, testing and production environments shall be separated and secured.	yes
ISMS A.8.32 PIMS 6.9.1.2 PIMS 6.11.2.2 PIMS 6.11.2.3 PIMS 6.11.2.4	Change Management	Changes to information processing facilities and information systems shall be subject to change management procedures.	yes

ISMS A.8.33 PIMS 6.11.3.1	Test information	Test information shall be appropriately selected, protected and managed.	yes
ISMS A.8.34 PIMS 6.9.7.1	Protection of information systems during audit testing	Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and appropriate management.	yes
ISO 27701:2019 Annex A (PII Controllers)			
Reference	**Control**	**Control description**	**Implemented**
A.7.2	**Conditions for collection and processing**		
A.7.2.1	Identify and document purpose	The organization shall identify and document the specific purposes for which the PII will be processed.	Yes
A.7.2.2	Identify lawful basis	The organization shall determine, document and	Yes

		comply with the relevant lawful basis for the processing of PII for the identified purposes.	
A.7.2.3	Determine when and how consent is to be obtained	The organization shall determine and document a process by which it can demonstrate if, when and how consent for the processing of PII was obtained from PII principals	Yes
A.7.2.4	Obtain and record consent	The organization shall obtain and record consent from PII principals according to the documented processes.	Yes
A.7.2.5	Privacy impact assessment	The organization shall assess the need for, and implement where appropriate, a privacy impact assessment whenever new processing of PII or changes to existing processing of PII is planned.	Yes
A.7.2.6	Contracts with PII processors	The organization shall have a written contract with any PII processor that it uses, and	Yes

		shall ensure that their contracts with PII processors address the implementation of the appropriate controls in Annex B.	
A.7.2.7	Joint PII controller	The organization shall determine respective roles and responsibilities for the processing of PII (including PII protection and security requirements) with any joint PII controller.	Yes
A.7.2.8	Records related to processing PII	The organization shall determine and securely maintain the necessary records in support of its obligations for the processing of PII.	Yes
A.7.3	**Obligations to PII principals**		
A.7.3.1	Determining and fulfilling obligations to PII principals	The organization shall determine and document their legal, regulatory and business obligations to PII principals related to the processing of	Yes

		their PII and provide the means to meet these obligations.	
A.7.3.2	Determining information for PII principals	The organization shall determine and document the information to be provided to PII principals regarding the processing of their PII and the timing of such a provision.	Yes
A.7.3.3	Providing information to PII principals	The organization shall provide PII principals with clear and easily accessible information identifying the PII controller and describing the processing of their PII.	Yes
A.7.3.4	Providing mechanism to modify or withdraw consent	The organization shall provide a mechanism for PII principals to modify or withdraw their consent.	Yes
A.7.3.5	Providing mechanism to object to PII processing	The organization shall provide a mechanism for PII principals to object to the processing of their PII.	Yes

A.7.3.6	Access, correction and/or erasure	The organization shall implement policies, processes and/or mechanisms to meet their obligations to PII principals to access, correct and/or erase their PII.	Yes
A.7.3.7	PII controllers' obligations to inform third parties	The organization shall inform third parties with whom PII has been shared of any modification, withdrawal or objections pertaining to the shared PII, and implement appropriate policies, processes and/ or mechanisms to do so.	Yes
A.7.3.8	Providing copy of PII processed	The organization shall be able to provide a copy of the PII that is processed when requested by the PII principal.	Yes
A.7.3.9	Handling requests	The organization shall define and document policies and processes for handling and responding to legitimate requests from PII principals.	Yes

A.7.3.10	Automated decision making	The organization shall identify and address obligations, including legal obligations, to the PII principals resulting from decisions made by the organization which are related to the PII principal based solely on automated processing of PII.	Yes
A.7.4	**Privacy by design and privacy by default**		
A.7.4.1	Limit collection	The organization shall limit the collection of PII to the minimum that is relevant, proportional and necessary for the identified purposes.	Yes
A.7.4.2	Limit processing	The organization shall limit the processing of PII to that which is adequate, relevant and necessary for the identified purposes.	Yes
A.7.4.3	Accuracy and quality	The organization shall ensure and document that PII is as accurate, complete and up-to-	Yes

		date as is necessary for the purposes for which it is processed, throughout the life-cycle of the PII.	
A.7.4.4	PII minimization objectives	The organization shall define and document data minimization objectives and what mechanisms (such as de-identification) are used to meet those objectives.	Yes
A.7.4.5	PII de-identification and deletion at the end of processing	The organization shall either delete PII or render it in a form which does not permit identification or re-identification of PII principals, as soon as the original PII is no longer necessary for the identified purpose(s).	Yes
A.7.4.6	Temporary files	The organization shall ensure that temporary files created as a result of the processing of PII are disposed of (e.g. erased or destroyed) following documented processes within	Yes

		a specified, documented period.	
A.7.4.7	Retention	The organization shall not retain PII for longer than is necessary for the purposes for which the PII is processed.	Yes
A.7.4.8	Disposal	The organization shall have documented policies, processes and/or mechanisms for the disposal of PII.	Yes
A.7.4.9	PII transmission controls	The organization shall subject PII transmitted (e.g. sent to another organization) over a data-transmission network to appropriate controls designed to ensure that the data reaches its intended destination.	Yes
A.7.5	**PII sharing, transfer, and disclosure**		
A.7.5.1	Identify basis for PII transfer between jurisdictions	The organization shall identify and document the relevant basis for transfers of PII between jurisdictions.	Yes

A.7.5.2	Countries and international organizations to which PII can be transferred	The organization shall specify and document the countries and international organizations to which PII can possibly be transferred.	Yes
A.7.5.3	Records of transfer of PII	The organization shall record transfers of PII to or from third parties and ensure cooperation with those parties to support future requests related to obligations to the PII principals.	Yes
A.7.5.4	Records of PII disclosure to third parties	The organization shall record disclosures of PII to third parties, including what PII has been disclosed, to whom and at what time.	Yes
ISO 27701:2019 Annex B (PII Processors)			
Reference	**Control**	**Control description**	**Implemented**

B.8.2	Conditions for collection and processing		
B.8.2.1	Customer agreement	The organization shall ensure, where relevant, that the contract to process PII addresses the organization's role in providing assistance with the customer's obligations (taking into account the nature of processing and the information available to the organization).	Yes
B.8.2.2	Organization's purposes	The organization shall ensure that PII processed on behalf of a customer are only processed for the purposes expressed in the documented instructions of the customer.	Yes
B.8.2.3	Marketing and advertising use	The organization shall not use PII processed under a contract for the purposes of marketing and advertising without establishing that prior consent was obtained from the appropriate PII principal. The	Yes

		organization shall not make providing such consent a condition for receiving the service.	
B.8.2.4	Infringing instruction	The organization shall inform the customer if, in its opinion, a processing instruction infringes applicable legislation and/or regulation.	Yes
B.8.2.5	Customer obligations	The organization shall provide the customer with the appropriate information such that the customer can demonstrate compliance with their obligations.	Yes
B.8.2.6	Records related to processing PII	The organization shall determine and maintain the necessary records in support of demonstrating compliance with its obligations (as specified in the applicable contract) for the processing of PII carried out on behalf of a customer.	Yes

B.8.3	**Obligations to PII principals**		
B.8.3.1	Obligations to PII principals	The organization shall provide the customer with the means to comply with its obligations related to PII principals.	Yes
B.8.4	**Privacy by design and privacy by default**		
B.8.4.1	Temporary files	The organization should ensure that temporary files created as a result of the processing of PII are disposed of (e.g. erased or destroyed) following documented procedures within a specified, documented period.	Yes
B.8.4.2	Return, transfer or disposal of PII	The organization shall provide the ability to return, transfer and/or disposal of PII in a secure manner. It shall also make its policy available to the customer.	Yes
B.8.4.3	PII transmission controls	The organization shall subject PII transmitted over a data-	Yes

		transmission network to appropriate controls designed to ensure that the data reaches its intended destination.	
B.8.5	**PII sharing, transfer, and disclosure**		
B.8.5.1	Basis for PII transfer between jurisdictions	The organization shall inform the customer in a timely manner of the basis for PII transfers between jurisdictions and of any intended changes in this regard, so that the customer has the ability to object to such changes or to terminate the contract.	Yes
B.8.5.2	Countries and international organizations to which PII can be transferred	The organization shall specify and document the countries and international organizations to which PII can possibly be transferred.	Yes

B.8.5.3	Records of PII disclosure to third parties	The organization shall record disclosures of PII to third parties, including what PII has been disclosed, to whom and when.	Yes
B.8.5.4	Notification of PII disclosure requests	The organization shall notify the customer of any legally binding requests for disclosure of PII.	Yes
B.8.5.5	Legally binding PII disclosures	The organization shall reject any requests for PII disclosures that are not legally binding, consult the corresponding customer before making any PII disclosures and accepting any contractually agreed requests for PII disclosures that are authorized by the corresponding customer.	Yes
B.8.5.6	Disclosure of subcontractors used to process PII	The organization shall disclose any use of subcontractors to process PII to the customer before use.	Yes

B.8.5.7	Engagement of a subcontractor to process PII	The organization shall only engage a subcontractor to process PII according to the customer contract.	Yes
B.8.5.8	Change of subcontractor to process PII	The organization shall, in the case of having general written authorization, inform the customer of any intended changes concerning the addition or replacement of subcontractors to process PII, thereby giving the customer the opportunity to object to such changes.	Yes