Présentation

Company	Shipfix Technologies SAS
Document Version	2
Purpose	Statement of Applicability
Valid from	13-Sep-21
Classification	Public

Statement of Applicability

		Applicable ?	Setup status	Reasons for selection: Risk Assessment Output	Legal and Regulatory Compliance	Contractual Obligation	Business Requirement	Best Practices	Justification	Proof
	ISO27001:2017 Statement of Applicability									
Controls	A.5 Information security policies									
	A.5.1 **Management direction for information security**									
	A.5.1.1 Policies for information security	✔	✔		✔	✔			To ensure our employee and relevant parties understand management direction and support for information security in accordance with business requirements and relevant laws and regulations.	Master List of Documents
	A.5.1.2 Review of the Policies for information security	✔	✔				✔	✔	To ensure the continuing suitability, adequacy and effectiveness of our policies.	Check Plan
	A.6 Organization of information security									
	A.6.1 **Internal organization**									
	A.6.1.1 Information Security roles & responsibilities	✔	✔			✔		✔	To ensure that everyone at Shipfix understand their roles and responsibilities and avoid possible doubt.	* Job Description available in Notion * Security and Privacy roles available for all in Security & Privacy Homepage
	A.6.1.2 Segregation of duties	✔	✔					✔	To reduce a) conflict of interests, b) opportunities for unauthorised or unintentional modification or misuse of the organization's assets.	* Shipfix has an org. chart (see Vanta) * Job des defined in @Our People * Roles available for all @Security & Privacy Homepage
	A.6.1.3 Contact with authorities	✔	✔		✔			✔	To be able to able to be reactive in case of crisis and to receive potential updates from the authorities related to security and privacy	* DPO registered as such with the CNIL
	A.6.1.4 Contact with special interest groups	✔	✔					✔	To be able to able to be reactive in case of crisis and to receive potential updates from the special interest groups related to security and privacy	* CFO Connect (HR / Finance / Legal)
	A.6.1.5 Information security in project management	✔	✔	✔			✔	✔	To ensure that Shipfix addresses Information Security and Privacy in project management, regardless of the type of the project.	Information Security Policy - Chapter 21. Security in Projects
	A.6.2 **Mobile devices and teleworking**									
	A.6.2.1 Mobile device policy	✔	✔				✔	✔	To manage the risks introduced by using mobile devices such as Laptops	Information Security Policy
	A.6.2.2 Teleworking	✔	✔	✔			✔	✔	To protect information accessed, processed or stored all all time and from any location given that the majority of our employees are teleworking	Information Security Policy
	A.7 Human resource security									
	A.7.1 **Prior to employment**									
	A.7.1.1 Screening	✔	✔	✔			✔		To ensure that employees are suitable for the roles for which they are considered.	Human Resource Security Policy
	A.7.1.2 Terms and conditions of employment	✔	✔				✔	✔	To ensure that employees and contractors understand their responsibilities.	Human Resource Security Policy
	A.7.2 **During employment**									
	A.7.2.1 Management responsibilities	✔	✔			✔		✔	To ensure management's involvement in Security and Privacy matters	Human Resource Security Policy
	A.7.2.2 Information security awareness, education and training	✔	✔	✔		✔		✔	To ensure our employees and other relevant third parties are aware of the security risks and understand how to avoid them	Human Resource Security Policy
	A.7.2.3 Disciplinary process	✔	✔	✔	✔			✔	To ensure employee understand that disciplinary process in place to take action against those who commit an information security and privacy breaches.	Human Resource Security Policy
	A.7.3 **Termination and change of employment**									
	A.7.3.1 Termination or change of employment responsibilities	✔	✔	✔			✔	✔	To ensure that information security and privacy responsibilities and duties remain valid after termination or change of employment.	Human Resource Security Policy
	A.8 Asset management									
	A.8.1 **Responsibility for assets**									
	A.8.1.1 Inventory of assets	✔	✔					✔	To identify clearly all our assets are be able to prioritise in case of security or privacy incident	Asset Management Policy
	A.8.1.2 Ownership of assets	✔	✔					✔	To identify organisational assets and define appropriate protection responsibilities.	Asset Management Policy
	A.8.1.3 Acceptable use of assets	✔	✔	✔				✔	To ensure appropriate use of assets by our employees or any other relevant third party	Asset Management Policy
	A.8.1.4 Return of assets	✔	✔	✔				✔	To ensure that we get back the assets upon departure of employees or relevant third parties to ensure privacy and security	Asset Management Policy
	A.8.2 **Information classification**									
	A.8.2.1 Classification of information	✔	✔	✔				✔	To ensure that information receives an appropriate level of protection in accordance with its importance to Shipfix.	Asset Management Policy
	A.8.2.2 Labelling of information	✔	✔	✔				✔	To make sure that anyone with access to informations understands easily its level of confidentiality	Asset Management Policy
	A.8.2.3 Handling of assets	✔	✔	✔				✔	To ensure that our employees and relevant third parties understands what are the security requirements relevant to each confidentiality classification	Asset Management Policy
	A.8.3 **Media handling**									
	A.8.3.1 Management of removable media	✔	✔	✔				✔	Because we do not restrict the use of removable media	Asset Management Policy
	A.8.3.2 Disposal of media	✔	✔	✔				✔	Because we do not restrict the use of removable media	Asset Management Policy
	A.8.3.3 Physical media transfer	✔	✔	✔				✔	Because we do not restrict the use of removable media	Asset Management Policy
	A.9 Access control									
	A.9.1 **Business requirements of access control**									
	A.9.1.1 Access control policy	✔	✔	✔			✔	✔	To limit access to our assets and informations systems	Access Control Policy
	A.9.1.2 Access to networks and network services	✔	✔	✔			✔	✔	To prevent misuse of our networks and related services (willingly or inadvertently)	Access Control Policy
	A.9.2 **User access management**									
	A.9.2.1 User registration and de-registration	✔	✔	✔			✔	✔	To monitor access rights	Access Control Policy
	A.9.2.2 User access provision	✔	✔	✔			✔	✔	To manage access rights	Access Control Policy
	A.9.2.3 Management of privileged access rights	✔	✔	✔			✔	✔	To prevent misuse of our systems (willingly or inadvertently)	Access Control Policy
	A.9.2.4 Management of secret authentication information of users	✔	✔	✔			✔	✔	To prevent unauthorised access to our systems	Access Control Policy
	A.9.2.5 Review of user access rights	✔	✔	✔			✔	✔	To ensure access are always up to date	Access Control Policy
	A.9.2.6 Removal or adjustment of access rights	✔	✔	✔			✔	✔	To prevent unauthorised access to our systems upon departure or change of responsibilities	Access Control Policy
	A.9.3 **User responsibilities**									
	A.9.3.1 Use of secret authentication information	✔	✔	✔				✔	To ensure understand the importance of strong authentication	Access Control Policy
	A.9.4 **System and application access control**									
	A.9.4.1 Information access restriction	✔	✔	✔				✔	To limit access to our systems	Access Control Policy
	A.9.4.2 Secure log-on procedures	✔	✔	✔				✔	To prevent unauthorized access to systems and applications.	Access Control Policy
	A.9.4.3 Password management system	✔	✔	✔				✔	To ensure the use of strong password	Access Control Policy
	A.9.4.4 Use of privileged utility programs	✔	✔	✔				✔	To restrict access to systems capable of overriding our informations and assets	Access Control Policy
	A.9.4.5 Access control to programme source code	✔	✔	✔				✔	To ensure we stay in control of our source code	Access Control Policy
	A.10 Cryptography									
	A.10.1 **Cryptographic controls (Policy is for all)**									
	A.10.1.1 Policy on the use of cryptography controls	✔	✔	✔	✔	✔	✔	✔	To ensure proper and effective use of cryptography	Cryptoography Policy
	A.10.1.2 Key management	✔	✔	✔	✔	✔	✔	✔	To ensure proper and effective use of cryptography	Cryptoography Policy
	A.11 Physical and environmental security									
	A.11.1 **Secure areas**									
	A.11.1.1 Physical security perimeter	✔	✔	✔	✔			✔	To give define the area with different types of restriction	Physical and Environment Security
	A.11.1.2 Physical entry controls	✔	✔	✔	✔			✔	To restrict access to our assets	Physical and Environment Security
	A.11.1.3 Securing offices, rooms and facilities	✔	✔	✔	✔			✔	To ensure the respective areas are secured appropriately	Physical and Environment Security
	A.11.1.4 Protecting against internal and environmental threats	✔	✔	✔	✔			✔	To ensure continuity in case of threats	Physical and Environment Security
	A.11.1.5 Working in secure areas	✔	✔	✔	✔			✔	To ensure the security of working areas	Physical and Environment Security
	A.11.1.6 Delivery and loading areas	✔	✔	✔	✔			✔	To restrict access to restricted areas	Physical and Environment Security
	A.11.2 **Equipment**									
	A.11.2.1 Equipment siting and protection	✔	✔	✔	✔			✔	To reduce the risks from environmental threats and hazards, and opportunities for unauthorised access	Physical and Environment Security
	A.11.2.2 Supporting utilities	✔	✔	✔	✔			✔	To ensure business continuity	Physical and Environment Security
	A.11.2.3 Cabling security	✔	✔	✔	✔			✔	To prevent interception, interference or damage of our assets	Physical and Environment Security
	A.11.2.4 Equipment maintenance	✔	✔	✔	✔			✔	To ensure business continuity	Physical and Environment Security
	A.11.2.5 Removal of assets	✔	✔	✔	✔			✔	To restrict the movements of assets	Physical and Environment Security
	A.11.2.6 Security of equipment and assets off-premises	✔	✔	✔	✔			✔	To ensure security of assets including off-premise (including when working from home)	Physical and Environment Security
	A.11.2.7 Secure disposal or re-use of equipment	✔	✔	✔	✔			✔	To prevent a data leak	Physical and Environment Security
	A.11.2.8 Unattended user equipment	✔	✔	✔	✔			✔	To prevent a data leak	Physical and Environment Security
	A.11.2.9 Clear desk and clear screen policy	✔	✔	✔	✔			✔	To prevent a data leak	Clean Desk Policy

A.12	Operations security									
A.12.1	Operational procedures and responsibilities									
A.12.1.1	Documented operating procedures	✔	✔	✔			✔	✔	To ensure secure operating activities	Information Security Policy
A.12.1.2	Change management	✔	✔	✔			✔	✔	To control changes to the organisation	Information Security Policy
A.12.1.3	Capacity management	✔	✔	✔			✔	✔	To ensure we have sufficient capacity at all time	Information Security Policy
A.12.1.4	Separation of development, testing and operational environments	✔	✔	✔			✔	✔	We work in separate environment to ensure unauthorised access to secure the operational environment	To add Security in Development Policy
A.12.2	Protection from malware									
A.12.2.1	Controls against malware	✔	✔	✔			✔	✔	To protect our IT environment	Information Security Policy
A.12.3	Backup									
A.12.3.1	Information back up	✔	✔	✔			✔	✔	To be able to restore the system at any point	Backup and recovery policy
A.12.4	Logging and monitoring									
A.12.4.1	Event logging	✔	✔	✔	✔		✔	✔	To track events in order to ensure traceability	Information Security Policy
A.12.4.2	Protection of log information	✔	✔	✔	✔		✔	✔	To ensure the integrity of our log data	Information Security Policy
A.12.4.3	Administrator and operator logs	✔	✔	✔	✔		✔	✔	To track event safeguard the integrity of changes	Information Security Policy
A.12.4.4	Clock synchronisation	✔	✔					✔	to ensure we have a single reference time to maintain a traceability of our events	Information Security Policy
A.12.5	Control of operational software									
A.12.5.1	Installation of software on operational systems	✔	✔					✔	Control software installation to ensure security of our system and enhanced traceability	Information Security Policy
A.12.6	Technical vulnerability management									
A.12.6.1	Management of technical vulnerabilities	✔	✔	✔				✔	To reinforces our systems and enhance availability	Information Security Policy
A.12.6.2	Restrictions on software installation	✔	✔	✔				✔	To manage the traceability of software installation	Information Security Policy
A.12.7	Information systems audit considerations									
A.12.7.1	Information systems audit controls	✔	✔					✔	To reinforce integrity via audit controls	Audit Policy
A.13	Communications Security									
A.13.1	Network security management									
A.13.1.1	Network controls	✔	✔					✔	Networks managements and controls will help to protect our information in systems and applications (availability)	Information Security Policy
A.13.1.2	Security of network controls	✔	✔	✔				✔	To reinforce the security, ensure consistent service levels of all network services (mostly outsourced) to enhanced security and availability	Information Security Policy
A.13.1.3	Segregation in networks	✔	✔					✔	To ensure the protection of information in networks	Information Security Policy
A.13.2	Information transfer									
A.13.2.1	Information transfer policies and procedures	✔	✔					✔	To protect the transfer of information.	Information Security Policy
A.13.2.2	Agreements on information transfer	✔	✔					✔	To secure transfer of business information between Shipfix and third-parties	Information Security Policy
A.13.2.3	Electronic messaging	✔	✔					✔	To protect our emails	Information Security Policy
A.13.2.4	Confidentiality or non-disclosure agreements	✔	✔					✔	To protect our trade and ensure confidentiality of our employees and third parties during and after their relationship with Shipfix	Information Security Policy
A.14	System acquisition, development and maintenance									
A.14.1	Security requirements of information systems									
A.14.1.1	Information security requirements analysis and specification	✔	✔	✔			✔	✔	So InfoSec requirements are included in the requirements for information systems	Secure Development Policy
A.14.1.2	Securing application services on public networks	✔	✔	✔			✔	✔	To be protected from fraudulent activity	Secure Development Policy
A.14.1.3	Protecting application services transactions	✔	✔	✔			✔	✔	To preserve the integrity of our data, systems and any other assets	Secure Development Policy
A.14.2	Security in development and support processes									
A.14.2.1	Secure development policy	✔	✔	✔			✔	✔	To explain clearly to everyone the security measure for secure development	Secure Development Policy
A.14.2.2	System change control procedures	✔	✔	✔			✔	✔	To secure and control the lifecycle of our development	Secure Development Policy
A.14.2.3	Technical review of applications after operating platform	✔	✔	✔			✔	✔	To ensure availability when operating platforms are changed	Secure Development Policy
A.14.2.4	Restrictions on changes to software	✔	✔	✔			✔	✔	To ensure integrity and traceability by limiting modifications to software packages to necessary changes	Secure Development Policy
A.14.2.5	Secure system engineering principles	✔	✔	✔			✔	✔	to reinforce the overall integrity of the platform	Secure Development Policy
A.14.2.6	Secure development environment	✔	✔	✔			✔	✔	To ensure that ISMSSec is designed and implemented within the development lifecycle of information systems	Secure Development Policy
A.14.2.7	Outsourced development	⃠							Shipfix does all development "in-house"	Secure Development Policy
A.14.2.8	System security testing	✔	✔	✔			✔	✔	Testing is necessary for the integrity of the platform	Secure Development Policy
A.14.2.9	System acceptance testing	✔	✔	✔			✔	✔	Testing is necessary for the integrity of the platform	Secure Development Policy
A.14.3	Test data									
A.14.3.1	Protection of test data	✔	✔	✔			✔	✔	To maintain traceability of test data	Secure Development Policy
A.15	Supplier relationships									
A.15.1	Information security in supplier relationships									
A.15.1.1	Information security policy for supplier relationships	✔	✔	✔			✔	✔	Because our suppliers are expected to have a similar level of security as we do	Third-Party Management Policy
A.15.1.2	Addressing security within supplier agreements	✔	✔	✔			✔	✔	To protect our assets from our suppliers	Third-Party Management Policy
A.15.1.3	Information and communication technology supply chain	✔	✔	✔			✔	✔	Because our suppliers are expected to have a similar level of security as we do	Third-Party Management Policy
A.15.2	Supplier service delivery management									
A.15.2.1	Monitoring and review of supplier services	✔	✔	✔			✔	✔	Because our suppliers are expected to have a similar level of security as we do	Third-Party Management Policy
A.15.2.2	Managing changes to supplier services	✔	✔	✔			✔	✔	To ensure a consistent and effective approach to security incidents	Third-Party Management Policy
A.16	Information security incident management									
A.16.1	Management of information security incidents and improvements									
A.16.1.1	Responsibilities and procedures	✔	✔	✔		✔	✔	✔	For a consistent security management of our third parties	Incident Response Plan
A.16.1.2	Reporting information security events	✔	✔	✔		✔	✔	✔	To ensure traceability of security events	Incident Response Plan
A.16.1.3	Reporting information security weaknesses	✔	✔	✔		✔	✔	✔	To ensure traceability of weaknesses so we can learn from them	Incident Response Plan
A.16.1.4	Assessment of and decision on information security events	✔	✔	✔		✔	✔	✔	To ensure we have the right and consistent classification for security events for a purpose of traceability	Incident Response Plan
A.16.1.5	Response to information security incidents	✔	✔	✔		✔	✔	✔	We need to response to incident according to the procedure to avoid confusion upon security incident	Incident Response Plan
A.16.1.6	Learning from information security incidents	✔	✔	✔		✔	✔	✔	To ensure continuous learning and improvement of our security and privacy systems	Incident Response Plan
A.16.1.7	Collection of evidence	✔	✔	✔		✔	✔	✔	To ensure traceability of events	Incident Response Plan
A.17	Information security aspects of business continuity management									
A.17.1	Information security continuity									
A.17.1.1	Planning information security continuity	✔	✔	✔		✔	✔	✔	To be prepared in case of incident and avoid confusion	Business Continuity Plan
A.17.1.2	Implementing information security continuity	✔	✔	✔		✔	✔	✔	To be prepared in case of incident and avoid confusion	Business Continuity Plan
A.17.1.3	Verify, review and evaluate information security continuity	✔	✔	✔		✔	✔	✔	To ensure that our information security continuity controls remain valid and effective during adverse situations.	Business Continuity Plan
A.17.2	Redundancies									
A.17.2.1	Availability of information processing facilities	✔	✔	✔		✔	✔	✔	To ensure availability of information processing facilities.	Business Continuity Plan
A.18	Compliance									
A.18.1	Compliance with legal and contractual requirements									
A.18.1.1	Identification of applicable legislation and contractual requirements	✔	✔	✔	✔	✔		✔	To avoid legal or contractual breaches at any time	Information Security Policy
A.18.1.2	Intellectual property rights	✔	✔	✔	✔	✔		✔	To avoid legal or contractual breaches at any time	Information Security Policy
A.18.1.3	Protection of records	✔	✔	✔	✔	✔		✔	To ensure the availability of records	Information Security Policy
A.18.1.4	Privacy and protection of personally identifiable information	✔	✔	✔	✔	✔		✔	To ensure the privacy and protection of PII for our clients and any other parties	Information Security Policy
A.18.1.5	Regulation of cryptographic controls	✔	✔	✔	✔	✔		✔	To ensure our cryptography remains in line with contractual and legal requirements	Information Security Policy
A.18.2	Information security reviews									
A.18.2.1	Independent review of information security	✔	✔	✔	✔	✔		✔	To have a third party perspective on our security and privacy systems	Information Security Policy
A.18.2.2	Compliance with security policies and standards	✔	✔	✔	✔	✔		✔	To ensure that the policies are applicable on all divisions	Information Security Policy
A.18.2.3	Technical compliance review	✔	✔	✔	✔	✔		✔	To ensure our policies are always up to date and in line with out technical organisation	Information Security Policy

ISO27701 Statement of Applicability

A.7	PIMS-specific reference control objectives and controls (PII Controllers)									
A.7.2	Conditions for collection and processing									
A.7.2.1	The organization shall identify and document the specific purposes for which the PII will be processed.	✔	✔	✔	✔				To identify and document the purposes for which PII are processed.	PIMS Policy - Data Controller
A.7.2.2	The organization shall determine, document and comply with the relevant lawful basis for the processing of PII for the identified purposes.	✔	✔	✔	✔				To ensure that our processing activities are legally authorised	PIMS Policy - Data Controller
A.7.2.3	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	✔	✔	✔	✔				To have a clear mapping on consent obtention	PIMS Policy - Data Controller
A.7.2.4	The organization shall obtain and record consent from PII principals according to the documented processes.	✔	✔	✔	✔				To ensure we retain record of consent for traceability purposes	PIMS Policy - Data Controller
A.7.2.5	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.	✔	✔	✔	✔				To assess if an impact assessment is required for existing processing activities and new ones	PIMS Policy - Data Controller
A.7.2.6	The organization shall have a written contract with any PII processor that it uses, and shall ensure that their contracts with PII processors address the implementation of the appropriate controls in Annex B.	✔	✔	✔	✔				To ensure that we maintain a consistent approach with our processors	PIMS Policy - Data Controller
A.7.2.7	The organization shall determine respective roles and responsibilities for the processing of PII (including PII protection and security requirements) with any joint PII controller.	✔		✔	✔				We are only joint controller with our UK entity with whom we singed a joint processing agreement	PIMS Policy - Data Controller
A.7.2.8	The organization shall determine and securely maintain the necessary records in support of its obligations for the processing of PII.	✔	✔	✔	✔				To maintain an up to date recording of processing activities	PIMS Policy - Data Controller
A.7.3	Obligations to PII principals									
A.7.3.1	The organization shall determine and document their legal, regulatory and business obligations to PII principals related to the processing of their PII and provide the means to meet these obligations.	✔	✔	✔	✔				To determine and document our legal, regulatory and business obligations to PII principals	PIMS Policy - Data Controller
A.7.3.2	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.	✔	✔	✔	✔				To ensure we provide the appropriate information to our PII principals	PIMS Policy - Data Controller

A.7.3.3	The organization shall provide PII principals with clear and easily accessible information identifying the PII controller and describing the processing of their PII.	✔	✔	✔	✔				To describe the information processed to PII principale and make sure that information is easilty available	PIMS Policy - Data Controller
A.7.3.4	The organization shall provide a mechanism for PII principals to modify or withdraw their consent.	✔	✔	✔	✔				To let PII principals amend their consent	PIMS Policy - Data Controller
A.7.3.5	The organization shall provide a mechanism for PII principals to object to the processing of their PII.	✔	✔	✔	✔				To provide a mechanism for PII principals to object to the processing of their PII.	PIMS Policy - Data Controller
A.7.3.6	The organization shall implement policies, procedures and/or mechanisms to meet their obligations to PII principals to access, correct and/or erase their PII.	✔	✔	✔	✔				To ensure we have the rights measure in place to let our PII principals to access, correct and/or erase their PII.	PIMS Policy - Data Controller
A.7.3.7	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, procedures and/or mechanisms to do so.	✔	✔	✔	✔				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, procedures and/or mechanisms to do so.	PIMS Policy - Data Controller
A.7.3.8	The organization shall be able to provide a copy of the PII that is processed when requested by the PII principal.	✔	✔	✔	✔				So PII principals can request a copy of the PII Processed	PIMS Policy - Data Controller
A.7.3.9	The organization shall define and document policies and procedures for handling and responding to legitimate requests from PII principals.	✔	✔	✔	✔				To have a consistent approach to responding to legitimate requests	PIMS Policy - Data Controller
A.7.3.10	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.	✔	✔	✔	✔				To address legal and contractual obligations related to the automated processing of PII.	PIMS Policy - Data Controller
A.7.4	**Privacy by design and privacy by default**									
A.7.4.1	The organization shall limit the collection of PII to the minimum that is relevant, proportional and necessary for the identified purposes.	✔	✔	✔	✔				Limit collection to what is necessary for the protection of our PII principals	PIMS Policy - Data Controller
A.7.4.2	The organization shall limit the processing of PII to that which is adequate, relevant and necessary for the identified purposes.	✔	✔	✔	✔				To limit the collection and processing to what is strictly necessary	PIMS Policy - Data Controller
A.7.4.3	The organization shall ensure and document that PII is as accurate, complete and up-to-date as is necessary for the purposes for which it is processed, throughout the life-cycle of the PII.	✔	✔	✔	✔				Accuracy and quality is paramount to ensure the integrity of our data	PIMS Policy - Data Controller
A.7.4.4	The organization shall define and document data minimization objectives and what mechanisms (such as de-identification) are used to meet those objectives.	✔	✔	✔	✔				To ensure we have a data minimisation strategy	PIMS Policy - Data Controller
A.7.4.5	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).	✔	✔	✔	✔				To delete PII data when no longer necessary	PIMS Policy - Data Controller
A.7.4.6	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 procedures within a specified, documented period	✔	✔	✔	✔				To ensure the safety of PII that could be present in temporary files	PIMS Policy - Data Controller
A.7.4.7	The organization shall not retain PII for longer than is necessary forthe purposes for which the PII is processed.	✔	✔	✔	✔				To minimise the period of retention of PII data	PIMS Policy - Data Controller
A.7.4.8	The organization shall have documented policies, procedures and/ or mechanisms for the disposal of PII	✔	✔	✔	✔				To clearly identify how we dispose of personal data	PIMS Policy - Data Controller
A.7.4.9	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.	✔	✔	✔	✔				To ensure that PII data reaches its intended destination and avoid breaches	PIMS Policy - Data Controller
A.7.5	**PII sharing, transfer and disclosure**									
A.7.5.1	The organization shall identify and document the relevant basis for transfers of PII between jurisdictions	✔	✔	✔	✔				data between jurisdictions	PIMS Policy - Data Controller
A.7.5.2	The organization shall specify and document the countries and international organizations to which PII can possibly be transferred	✔	✔	✔	✔				The have a clear understanding of the countries and international organizations to which PII can possibly be transferred.	PIMS Policy - Data Controller
A.7.5.3	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.	✔	✔	✔	✔				We maintain a record of 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.	PIMS Policy - Data Controller
A.7.5.4	The organization shall record disclosures of PII to third parties, including what PII has been disclosed, to whom and at what time.	✔	✔	✔	✔				To have a system which ensure the traceability of our actions	PIMS Policy - Data Controller

B.8	**PIMS-specific reference control objectives and controls (PII Processors)**									
B.8.2	**Conditions for collection and processing**									
B.8.2.1	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).	✔	✔	✔	✔				We need to be able to provide assistance with the customer's obligations	PIMS Policy - Data Processor
B.8.2.2	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.	✔	✔	✔	✔				We need to guarantee to our clients that we only process PII in line with the agreement	PIMS Policy - Data Processor
B.8.2.3	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 organization shall not make providing such consent a condition for receiving the service	✔	✔	✔	✔				We must 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	PIMS Policy - Data Processor
B.8.2.4	The organization shall inform the customer if, in its opinion, a processing instruction infringes applicable legislation and/or regulation.	✔	✔	✔	✔				We need to inform the customer if, in our opinion, a processing instruction infringes applicable legislation and/or regulation.	PIMS Policy - Data Processor
B.8.2.5	The organization shall provide the customer with the appropriate information such that the customer can demonstrate compliance with their obligations.	✔	✔	✔	✔				We need to be able to assist our customers to meet their obligations	PIMS Policy - Data Processor
B.8.2.6	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.	✔	✔	✔	✔				We maintain a record to support our compliance with our obligations when processing PII	PIMS Policy - Data Processor
B.8.3	**Obligations to PII principals**									
B.8.3.1	The organization shall provide the customer with the means to comply with its obligations related to PII principals.	✔	✔	✔	✔				We must provide our customer with the means to comply with its obligations related to PII principals.	PIMS Policy - Data Processor
B.8.4	**Privacy by design and privacy by default**									
B.8.4.1	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 procedures within a specified, documented period.	✔	✔	✔	✔				To ensure the safety of PII that could be present in temporary files	PIMS Policy - Data Processor
B.8.4.2	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.	✔	✔	✔	✔				To ensure that we have the ability to return, transfer and/or disposal of PII in a secure manner and that our customers have access to the relevant policy	PIMS Policy - Data Processor
B.8.4.3	The organization shall subject PII transmitted over a data-transmission network to appropriate controls designed to ensure that the data reaches its intended destination.	✔	✔	✔	✔				To ensure PII data are transmitted in a controlled environment	PIMS Policy - Data Processor
B.8.5	**PII sharing, transfer and disclosure**									
B.8.5.1	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.	✔	✔	✔	✔				To determine when it is justifiable to transfer data between jurisdictions	PIMS Policy - Data Processor
B.8.5.2	The organization shall specify and document the countries and international organizations to which PII can possibly be transferred.	✔	✔	✔	✔				The have a clear understanding of the countries and international organisations to which PII can possibly be transferred.	PIMS Policy - Data Processor
B.8.5.3	The organization shall record disclosures of PII to third parties, including what PII has been disclosed, to whom and when.	✔	✔	✔	✔				We maintain a record of 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.	PIMS Policy - Data Processor
B.8.5.4	The organization shall notify the customer of any legally binding requests for disclosure of PII.	✔	✔	✔	✔				To notify PII subject when we have a legally binding request for disclosure (when authorised to disclose)	PIMS Policy - Data Processor
B.8.5.5	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.	✔	✔	✔	✔				So we know when to reject PII data disclosure request (when not legally binding)	PIMS Policy - Data Processor
B.8.5.6	The organization shall disclose any use of subcontractors to process PII to the customer before use	✔	✔	✔	✔				To ensure transparency of subcontractors	PIMS Policy - Data Processor
B.8.5.7	The organization shall only engage a subcontractor to process PII according to the customer contract.	✔	✔	✔	✔				To ensure we stay in compliance with our contractual obligations	PIMS Policy - Data Processor
B.8.5.8	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.	✔	✔	✔	✔				Let customer know about changes concerning the addition or replacement of subcontractors to process PII, thereby giving the opportunity to object to such changes.	PIMS Policy - Data Processor