

## TECHNICAL AND ORGANIZATIONAL MEASURES

This Exhibit forms part of the DPA. Capitalized terms not defined in this Exhibit have the meaning set forth in this DPA.

The Company has implemented technical and organizational security measures which are consistent with industry standards, including ISO 27001, 27017, 27018 and 27701.<sup>1</sup> The Company Information Security & Privacy Management System (ISMS) ensures continued operation of sure measures, and supports the governance of information security and processing of Personal Data as a PII processor across all global locations and cloud services and is inclusive of the following sites with primary security operations:

- Musarubra US, LLC. - 6000 Headquarters Drive, Suite 600, Plano, TX 75024, USA.
- Musarubra Ireland Limited - Building 2000, Citygate, Mahon, Cork City, Ireland, T12RRC9.

In addition to any data security requirements set forth in the DPA, the Company shall comply with the following, as derived from industry standards:

Standard	Control Ref/ Title		Control Description
<b>ISO 27001 - Information Security Management System</b>  <i>(incl. controls amendments for ISO 27017/27018/27701)</i>	<b><i>6.1.3 - A.5 Information Security Policy</i></b>		
	5.1.1	Policies for information security	A set of policies for information security is defined, approved by management, published, and communicated to employees and relevant external parties.
	5.1.2	Review of the policies for information security	The policies for information security are reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.
	<b><i>6.1.3 - A.6 Organization of Information Security</i></b>		
	6.1.1	Information security roles and responsibilities	All information security responsibilities are defined and allocated.
	6.1.2	Segregation of duties	Conflicting duties and areas of responsibility are segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.
	6.1.3	Contact with authorities	Appropriate contacts with relevant authorities are maintained.
	6.1.4	Contact with special interest groups	Appropriate contacts with special interest groups or other specialist security forums and professional associations are maintained.

Standard	Control Ref/ Title		Control Description
	6.1.5	Information security in project management	Information security is addressed in project management, regardless of the type of the project.
	6.2.1	Mobile device policy	A policy and supporting security measures is adopted to manage the risks introduced by using mobile devices.
	6.2.3	Teleworking	A policy and supporting security measures is implemented to protect information accessed, processed, or stored at teleworking sites.
	<b>6.1.3 - A.7 Human Resource Security</b>		
	7.1.1	Screening	Background verification checks on all candidates for employment is carried out in accordance with relevant laws, regulations and ethics and is proportional to the business requirements, the classification of the information to be accessed and the perceived risks.
	7.1.2	Terms and conditions of employment	The contractual agreements with employees and contractors state their and the organization's responsibilities for information security.
	7.2.1	Management responsibilities	Management requires all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.
	7.2.2	Information security awareness, education, training	All employees of the organization and, where relevant, contractors receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.
	7.2.3	Disciplinary process	There is a formal and communicated disciplinary process in place to act against employees who have committed an information security breach.
	7.3.1	Termination or change of	Information security responsibilities and duties that remain valid after termination or change of employment

Standard	Control Ref/ Title		Control Description
		employment responsibilities	are defined, communicated to the employee or contractor, and enforced.
	<b>6.1.3 - A.8 Asset Management</b>		
	8.1.1	Inventory of assets	Assets associated with information and information processing facilities are identified and an inventory of these assets shall be drawn up and maintained.
	8.1.2	Ownership of assets	Assets maintained in the inventory are owned.
	8.1.3	Acceptable use of assets	Rules for the acceptable use of information and of assets associated with information and information processing facilities are identified, documented, and implemented.
	8.1.4	Return of assets	All employees and external party users return all the organizational assets in their possession upon termination of their employment, contract, or agreement.
	8.2.1	Classification of information	Information is classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.
	8.2.2	Labelling of information	An appropriate set of procedures for information labelling is developed and implemented in accordance with the information classification scheme adopted by the organization.
	8.2.3	Handling of assets	Procedures for handling assets is developed and implemented in accordance with the information classification scheme adopted by the organization.
	8.3.1	Management of removal media	Procedures is implemented for the management of removable media in accordance with the classification scheme adopted by the organization.
	8.3.2	Disposal of media	Media is disposed of securely when no longer required, using formal procedures.

Standard	Control Ref/ Title		Control Description
	8.3.3	Physical media transfer	Media containing information is protected against unauthorized access, misuse, or corruption during transportation.
	<b>6.1.3 - A.9 Access Control</b>		
	9.1.1	Access control policy	An access control policy is established, documented, and reviewed based on business and information security requirements.
	9.1.2	Access to networks and network services	Users are only provided with access to the network and network services if they have been specifically authorized to use such services.
	9.2.1	User registration and de-registration	A formal user registration and de-registration process is implemented to enable assignment of access rights.
	9.2.2	User access provisioning	A formal user access provisioning process is implemented to assign or revoke access rights for all user types to all systems and services.
	9.2.3	Management of privileged access rights	The allocation and use of privileged access rights is restricted and controlled.
	9.2.4	Management of secret authentication info of users	The allocation of secret authentication information is controlled through a formal management process.
	9.2.5	Review of user access rights	Asset owners review users' access rights at regular intervals.
	9.2.6	Removal or adjustment of access rights	The access rights of all employees and external party users to information and information processing facilities are removed upon termination of their employment, contract, or agreement, or adjusted upon change.
	9.3.1	Use of secret authentication information	Users are required to follow the organization's practices in the use of secret authentication information.
9.4.1	Information access restriction	Access to information and application system functions is restricted in accordance with the access control policy.	

Standard	Control Ref/ Title		Control Description	
	9.4.2	Secure log on procedures	Where required by the access control policy, access to systems and applications is controlled by a secure log-on procedure.	
	9.4.3	Password management system	Password management systems is interactive and ensures quality passwords.	
	9.4.4	Use of privileged utility programs	The use of utility programs that might be capable of overriding system and application controls is restricted and tightly controlled.	
	9.4.5	Access control to program source code	Access to program source code is restricted.	
	<b>6.1.3 - A.10 Cryptography</b>			
	10.1.1	Policy on the use of cryptographic controls	A policy on the use of cryptographic controls for protection of information is developed and implemented.	
	10.1.2	Key management	A policy on the use, protection and lifetime of cryptographic keys is developed and implemented through their whole lifecycle.	
	<b>6.1.3 - A.11 Physical and Environmental Security</b>			
	11.1.1	Physical security perimeter	Security perimeters is defined and used to protect areas that contain either sensitive or critical information and information processing facilities.	
	11.1.2	Physical entry controls	Secure areas are protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	
	11.1.3	Securing offices, rooms, facilities	Physical security for offices, rooms and facilities are designed and applied.	
	11.1.4	Protecting against external and environmental threats	Physical protection against natural disasters, malicious attack or accidents are designed and applied.	
	11.1.5	Working in secure areas	Procedures for working in secure areas are designed and applied.	
	11.1.6	Delivery and loading areas	Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises are controlled and, if	

Standard	Control Ref/ Title		Control Description	
			possible, isolated from information processing facilities to avoid unauthorized access.	
	11.2.1	Equipment siting and protection	Equipment is sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.	
	11.2.2	Supporting utilities	Equipment is protected from power failures and other disruptions caused by failures in supporting utilities.	
	11.2.3	Cabling security	Power and telecommunications cabling carrying data or supporting information services are protected from interception, interference, or damage.	
	11.2.4	Equipment maintenance	Equipment are correctly maintained to ensure its continued availability and integrity.	
	11.2.5	Removal of assets	Equipment, information, or software are not taken off-site without prior authorization.	
	11.2.6	Security of equipment and assets off-premises	Security is applied to off-site assets considering the different risks of working outside the organization's premises.	
	11.2.7	Secure disposal or reuse of equipment	All items of equipment containing storage media is verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	
	11.2.8	Unattended user equipment	Users ensure that unattended equipment has appropriate protection.	
	11.2.9	Clear desk and clear screen policy	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities is adopted.	
	<b>6.1.3 - A.12 Operations Security</b>			
	12.1.1	Documented operating procedures	Operating procedures are documented and made available to all users who need them.	
12.1.2	Change management	Changes to the organization, business processes, information processing		

Standard	Control Ref/ Title		Control Description
			facilities and systems that affect information security are controlled.
	12.1.3	Capacity management	The use of resources is monitored, tuned and projections made of future capacity requirements to ensure the required system performance.
	12.1.4	Separation of development, testing & operational environments	Development, testing, and operational environments are separated to reduce the risks of unauthorized access or changes to the operational environment.
	12.2.1	Controls against malware	Detection, prevention, and recovery controls to protect against malware are implemented, combined with appropriate user awareness.
	12.3.1	Information backup	Backup copies of information, software and system images are taken and tested regularly in accordance with an agreed backup policy.
	12.4.1	Event logging	Event logs recording user activities, exceptions, faults and information security events are produced, kept and regularly reviewed.
	12.4.2	Protection of log information	Logging facilities and log information are protected against tampering and unauthorized access
	12.4.3	Administrator and operator logs	System administrator and system operator activities are logged, and the logs are protected and regularly reviewed.
	12.4.4	Clock synchronization	The clocks of all relevant information processing systems within an organization or security domain are synchronized to a single reference time source.
	12.5.1	Installation of software on operational systems	Procedures are implemented to control the installation of software on operational systems.
	12.6.1	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems being used are obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and

Standard	Control Ref/ Title		Control Description
			appropriate measures taken to address the associated risk.
	12.6.2	Restrictions on software installation	Rules governing the installation of software by users are established and implemented.
	12.7.1	Information systems audit controls	Audit requirements and activities involving verification of operational systems are carefully planned and agreed to minimize disruptions to business processes.
	<b>6.1.3 - A.13 Communications Security</b>		
	13.1.1	Network controls	Networks are managed and controlled to protect information in systems and applications.
	13.1.2	Security of network services	Security mechanisms, service levels and management requirements of all network services are identified and included in network services agreements, whether these services are provided in-house or outsourced.
	13.1.3	Segregation in networks	Groups of information services, users and information systems are segregated on networks.
	13.2.1	Information transfer policies and procedures	Formal transfer policies, procedures and controls are in place to protect the transfer of information using all types of communication facilities.
	13.2.2	Agreements on information transfer	Agreements address the secure transfer of business information between the organization and external parties.
	13.2.3	Electronic messaging	Information involved in electronic messaging is appropriately protected.
	13.2.4	Confidentiality or nondisclosure agreements	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information are identified, regularly reviewed, and documented.
	<b>6.1.3 - A.14 System Acquisition, Dev. &amp; Maintenance</b>		



Standard	Control Ref/ Title		Control Description
	14.1.1	Information security requirements analysis & specification	The information security related requirements are included in the requirements for new information systems or enhancements to existing information systems.
	14.1.2	Securing application services on public networks	Information involved in application services passing over public networks is protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.
	14.1.3	Protecting application services transactions	Information involved in application service transactions is protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.
	14.2.1	Secure development policy	Rules for the development of software and systems are established and applied to developments within the organization.
	14.2.2	System change control procedures	Changes to systems within the development lifecycle are controlled using formal change control procedures.
	14.2.3	Technical review of applications after operating platform changes	When operating platforms are changed, business critical applications are reviewed and tested to ensure there is no adverse impact on organizational operations or security.
	14.2.4	Restrictions on changes to software packages	Modifications to software packages are discouraged, limited to necessary changes and all changes are strictly controlled.
	14.2.5	Secure system engineering principles	Principles for engineering secure systems are established, documented, maintained, and applied to any information system implementation efforts.
	14.2.6	Secure development environment	secure development environments are established and are appropriately protected for system development and integration efforts to cover the entire system development lifecycle

Standard	Control Ref/ Title		Control Description
	14.2.7	Outsourced development	The organization supervises and monitors the activity of outsourced system development.
	14.2.8	System security testing	Testing of security functionality is carried out during development.
	14.2.9	System acceptance testing	Acceptance testing programs and related criteria are established for new information systems, upgrades, and new versions.
	14.3.1	Protection of test data	Test data is selected carefully, protected, and controlled.
	<b>6.1.3 - A.15 Supplier Relationship</b>		
	15.1.1	Information security policy for supplier relationships	Information security requirements for mitigating the risks associated with supplier's access to the organization's assets are agreed with the supplier and documented.
	15.1.2	Addressing security within supplier agreements	All relevant information security requirements are established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information
	15.1.3	Information communication technology supply chain	Agreements with suppliers include requirements to address the information security risks associated with information and communications technology services and product supply chain.
	15.2.1	Monitoring and review of supplier services	Supplier service delivery is regularly monitored, reviewed, and audited.
	15.2.2.	Managing changes to supplier services	Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures, and controls, are managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.
<b>6.1.3 - A.16.1.3 Information Security Incident Management</b>			

Standard	Control Ref/ Title		Control Description	
	16.1.1	Responsibilities and procedures	Management responsibilities and procedures are established to ensure a quick, effective, and orderly response to information security incidents.	
	16.1.2	Reporting information security events	Information security events are reported through appropriate management channels as quickly as possible.	
	16.1.3	Reporting information security weaknesses	Employees and contractors using the organization's information systems and services are required to note and report any observed or suspected information security weaknesses in systems or services.	
	16.1.4	Assessment of and decision on information security events	Information security events are assessed and are decided if they are to be classified as information security incidents.	
	16.1.5	Response to information security incidents	Information security incidents are responded to in accordance with the documented procedures.	
	16.1.6	Learning from information security incidents	Knowledge gained from analysing and resolving information security incidents are used to reduce the likelihood or impact of future incidents.	
	16.1.7	Collection of evidence	Procedures for the identification, collection, acquisition, and preservation of information, which can serve as evidence are defined and applicable.	
	<b>6.1.3 - A.17 Information Security Aspects of Business Continuity Management</b>			
	17.1.1	Planning information security continuity	Requirements for information security and the continuity of information security management in adverse situations, e.g., during a crisis or disaster are determined.	
	17.1.2	Implementing information security continuity	Processes and procedures and controls to ensure the required level of continuity for information security during an adverse situation are established, documented, implemented, and maintained.	

Standard	Control Ref/ Title		Control Description
	17.1.3	Verify, review, and evaluate information security continuity	Established and implemented information security continuity controls are verified at regular intervals in order to ensure that they are valid and effective during adverse situations.
	17.2.1	Availability of information processing facilities	Information processing facilities are implemented with redundancy sufficient to meet availability requirements.
	<b>6.1.3 - A.18 Compliance</b>		
	18.1.1	Identification of applicable legislation & contractual requirements	All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements are explicitly identified, documented, and kept up to date for each information system and the organization.
	18.1.2	Intellectual property rights	Appropriate procedures are implemented to ensure compliance with legislative, regulatory, and contractual requirements related to intellectual property rights and use of proprietary software products.
	18.1.3	Protection of records	Records are protected from loss, destruction, falsification, unauthorized access, and unauthorized release, in accordance with legislation, regulatory, contractual, and business requirements.
	18.1.4	Privacy and protection of Personal Data	Privacy and protection of personally identifiable information (Personal Data) are ensured as required in relevant legislation and regulation where applicable.
	18.1.5	Regulation of cryptographic controls	Cryptographic controls are used in compliance with all relevant agreements, legislation, and regulations.
	18.2.1	Independent review of information security	The organization's approach to managing information security and its implementation (i.e., control objectives, controls, policies, processes, and procedures for

Standard	Control Ref/ Title		Control Description
			information security) are reviewed independently at planned intervals or when significant changes occur.
	18.2.2	Compliance with security policies & standards	Managers regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards, and any other security requirements.
	18.2.3	Technical compliance review	Information systems are regularly reviewed for compliance with the organization's information security policies and standards
<b>ISO 27017 - Security Controls for Cloud Services</b>	<b>CLD.6.3 - Relationship between cloud service customer &amp; provider</b>		
	6.3.1	Shared roles & responsibilities within a cloud computing environment	Responsibilities for shared information security roles in the use of the cloud service are allocated to identified parties, documented, communicated, and implemented by both the cloud service customer and the cloud service provider.
	8.1.5	Removal of cloud service customer assets	Removal of cloud service customer assets
	<b>CLD.9.5 - Access control of CSP data in shared virtual environment</b>		
	9.5.1	Segregation in virtual computing environments	A cloud service customer's virtual environment running on a cloud service is protected from other cloud service customers and unauthorized persons.
	9.5.2	Virtual machine hardening	Virtual machines in a cloud computing environment are hardened to meet business needs.
	12.1.5	Administrator's operational security	Procedures for administrative operations of a cloud computing environment are defined, documented, and monitored.
	12.4.5	Monitoring of cloud services	The cloud service customer has the capability to monitor specified aspects of the operation of the cloud services that the cloud service customer uses.

Standard	Control Ref/ Title		Control Description
	13.1.4	Alignment of security management for virtual and physical networks	Upon configuration of virtual networks, consistency of configurations between virtual and physical networks is verified based on the cloud service provider's network security policy.
<b>ISO 27018 - Protection of Personal Data in Public Clouds, Acting as Personal Data Processors</b>	<b>A.2 - Consent and choice</b>		
	A.2.1	Obligation to cooperate regarding Personal Data principals' rights	The public cloud Personal Data processor can provide the cloud service customer with the means to enable them to fulfil their obligation to facilitate the exercise of Personal Data principals' rights to access, correct and/or erase Personal Data pertaining to them.
	<b>A.3 - Purpose legitimacy and specification</b>		
	A.3.1	Public cloud Personal Data processor's purpose	Personal Data to be processed under a contract is not processed for any purpose independent of the instructions of the cloud service customer.
	A.3.2	Public cloud Personal Data processor's commercial use	Personal Data processed under a contract is not used by the public cloud Personal Data processor for the purposes of marketing and advertising without express consent. Such consent is not a condition of receiving the service
	<b>A.5 - Data minimization</b>		
	A.5.1	Secure erasure of temporary files	Temporary files and documents are erased or destroyed within a specified, documented period
	<b>A.6 - Use, retention, and disclosure limitation</b>		
	A.6.1	Personal Data disclosure notification	The contract between the public cloud Personal Data processor and the cloud service customer requires the public cloud Personal Data processor to notify the cloud service customer, in accordance with any procedure and time periods agreed in the contract, of any legally binding request for disclosure of Personal Data by a law enforcement authority, unless such a disclosure is otherwise prohibited

Standard	Control Ref/ Title		Control Description
	A.6.2	Recording of Personal Data disclosure	Disclosures of Personal Data to third parties is recorded, including what Personal Data has been disclosed, to whom and at what time.
	<b>A.8 - Openness, transparency, and notice</b>		
	A.8.1	Disclosure of sub-contracted Personal Data processing	The use of sub-contractors by the public cloud Personal Data processor to process Personal Data is disclosed to the relevant cloud service customers before their use.
	<b>A.10 - Accountability</b>		
	A.10.1	Notification of a data breach involving Personal Data	The public cloud Personal Data processor promptly notifies the relevant cloud service customer in the event of any unauthorized access to Personal Data or unauthorized access to processing equipment or facilities resulting in loss, disclosure, or alteration of Personal Data.
	A.10.2	Retention period for administrative security policies and guidelines	Copies of security policies and operating procedures are retained for a specified, documented period upon replacement (including updating).
	A.10.3	Personal Data return, transfer, and disposal	The public cloud Personal Data processor have a policy in respect of the return, transfer and/or disposal of Personal Data and make this policy available to the cloud service customer
	<b>A.11 - Information security</b>		
	A.11.1	Confidentiality or non-disclosure agreements	Individuals under the public cloud Personal Data processor's control with access to Personal Data are subject to a confidentiality obligation.
	A.11.2	Restriction of the creation of hardcopy material	The creation of hardcopy material displaying Personal Data is restricted.
	A.11.3	Control and logging of data restoration	There is a procedure for, and a log of, data restoration efforts.
	A.11.4	Protecting data on storage media leaving the premises	Personal Data on media leaving the organization's premises is subject to an authorization procedure and is not accessible to anyone other than

Standard	Control Ref/ Title		Control Description
			authorized personnel (e.g., by encrypting the data concerned).
	A.11.5	Use of unencrypted portable storage media and devices	Portable physical media and portable devices that do not permit encryption cannot be used except where it is unavoidable, and any use of such portable media and devices is documented.
	A.11.6	Encryption of Personal Data transmitted over public data-transmission networks	Personal Data that is transmitted over public data-transmission networks is encrypted prior to transmission
	A.11.7	Secure disposal of hardcopy materials	Where hardcopy materials are destroyed, they are destroyed securely using mechanisms such as cross-cutting, shredding, incinerating, pulping, etc.
	A.11.8	Unique use of user IDs	If more than one individual has access to stored Personal Data, then they each have a distinct user ID for identification, authentication, and authorization purposes
	A.11.9	Records of authorized users	An up-to-date record of the users or profiles of users who have authorized access to the information system is maintained.
	A.11.10	User ID management	De-activated or expired user IDs are not granted to other individuals.
	A.11.11	Contract measures	Contracts between the cloud service customer and the public cloud Personal Data processor specify minimum technical and organizational measures to ensure that the contracted security arrangements are in place and that data are not processed for any purpose independent of the instructions of the controller. Such measures are not subject to unilateral reduction by the public cloud Personal Data processor
	A.11.12	Sub-contracted Personal Data processing	Contracts between the public cloud Personal Data processor and any sub-contractors that process Personal Data



Standard	Control Ref/ Title		Control Description
			specify minimum technical and organizational measures that meet the information security and Personal Data protection obligations of the public cloud Personal Data processor. Such measures are not subject to unilateral reduction by the sub-contractor.
	A.11.13	Access to data on pre-used data storage space	The public cloud Personal Data processor ensures that whenever data storage space is assigned to a cloud service customer, any data previously residing on that storage space is not visible to that cloud service customer.
	<b>A.12 - Privacy compliance</b>		
	A.12.1	Geographical location of Personal Data	The public cloud Personal Data processor specifies and document the countries in which Personal Data might possibly be stored.
	A.12.2	Intended destination of Personal Data	Personal Data transmitted using a data-transmission network is subject to appropriate controls designed to ensure that data reaches its intended destination.
<b>ISO 27701 – Privacy Information Management System</b>	<b>B.8.2 – Conditions for collection and processing</b>		
	<b>B.8.2.1</b>	Customer agreement	The organization shall ensure, where relevant, that the contract to process PII addresses the organization’s role in aiding with the customer’s obligations, (considering the nature of processing and the information available to the organization).
	<b>B.8.2.2</b>	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.
	<b>B.8.2.3</b>	Marketing and advertising use	The organization should 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 should not make providing such consent a condition for receiving the service.

Standard	Control Ref/ Title		Control Description	
	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	
	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.	
	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.	
	<b>B.8.3 – Obligations to PII principals</b>			
	B.8.3.1	Obligations to PII principals	The organization shall provide the customer with the means to comply with its obligations relating to PII principals	
	<b>B.8.4 – Privacy by design and privacy by default</b>			
	B.8.4.1	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 procedures within a specified, documented period.	
	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.	
	B.8.4.3	PII transmission controls	The organization shall subject PII transmitted over a data-transmission network to appropriate controls designed to ensure that the data reaches its intended destination.	
	<b>B.8.5 PII sharing, transfer and disclosure</b>			
	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	

Standard	Control Ref/ Title		Control Description
			changes in this regard, so that the customer could object to such changes or to terminate the contract.
	<b>B.8.5.2</b>	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.
	<b>B.8.5.3</b>	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.
	<b>B.8.5.4</b>	Notification of PII disclosure requests	The organization shall notify the customer of any legally binding requests for disclosure of PII.
	<b>B.8.5.5</b>	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.
	<b>B.8.5.6</b>	Disclosure of sub-contractors used to process PII	The organization shall disclose any use of subcontractors to process PII to the customer before use.
	<b>B.8.5.7</b>	Engagement of a subcontractor to process PII	The organization shall only engage a subcontractor to process PII according to the customer contract.
	<b>B.8.5.8</b>	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.

<sup>1</sup> The Company has recently undergone changes in organizational structure; and ISO certifications were non-transferable as part of the transaction. The Company’s predecessor has maintained ISO certifications since 2011 and has consistently remained compliant throughout our previous organizational changes. We continue to remain committed to maintaining industry accreditation with our established Certification Body Schellman & Company, LLC.