Statement of Applicability @ Digidentity

Controls Annex ISO27...

Title	Statement of Applicability - Controls Annex ISO27...
Date	1 July 2025
Version	2025-v1
Location	https://www.digidentity.eu/en/documentation/
Classification	Public

Revisions

Version	Date	Changes Made
2018-v1	26 September 2018	Initial version
2019-v1	1 June 2019	Clause A.14.2.7 changed to applicable
2020-v1	30 June 2020	Clause A.14.2.7 changed to not applicable
2021-v1	1 September 2021	Added ISO27701, ISO27017, ISO27018
2022-v1	1 June 2022	ISO27001: Clause A.14.2.7 changed to applicable
2023-v1	1 July 2023	Updated to ISO27001:2022
2024-v1	25 July 2024	Annual review - minor changes
2025-v1	1 July 2025	Certification marks updated to DNV, updated justification of controls

(*) All changes are marked in grey highlight.

07 Oct 2025
Den Haag

Digidentity B.V.
QUALIFIED BUSINESS SEAL

Contents

Statement of Applicability

A requirement of ISO27001:2022 (ISMS) is to produce a Statement of Applicability that contains the necessary controls and justification for inclusions, whether they are implemented or not, and the justification for inclusion (legal, contract or risk) and for exclusions of controls from Annex A.

Standards ISO27017:2015 (Security in Cloud), ISO27018:2019 (Personal Data in Cloud) and ISO27701:2019 (PIMS) require the extension of the ISO27001:2022 Statement of Applicability with the controls from each Annex of these standards.

This Statement of Applicability contains all the controls from Annex A of ISO27001:2022, Annex A of ISO27017:2021, Annex A of ISO27018:2020 and Annex A and Annex B of ISO27701:2019 with justification for inclusion or exclusion.

Justification of the controls selected is based on requirements from:

- Laws, Regulation or Standards (GDPR, eIDAS, NIS2, DORA, ISO27001:2022, ISO27017:2015, ISO27018:2019, ISO27701:2019, ISO22301:2019, ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2, ETSI TS 119 461, Afsprakenstelsel eTD (Dutch Trust Framework), PKIoverheid Program of Requirements and DIATF)
- Contractual Agreements with corporate customers and suppliers
- Risk Assessment performed by Digidentity (document: Risk Analysis 2025 @ DDY)

Digidentity has selected all controls from all standards except:

Standard	Section	Clause	Justification
ISO27017:2015	Annex A	CLD.13.1.4	Cloud Service Provider does not have a network security policy
ISO27701:2019	Annex A	A.7.2.7	Digidentity is not a joint controller
ISO27701:2019	Annex A	A.7.3.7	DDY does not use third parties that need to be informed

INFORMATION SECURITY MANAGEMENT SYSTEM
DNV
ISO/IEC 27001

INFORMATION SECURITY MANAGEMENT SYSTEM
DNV
ISO/IEC 27001
WITH EXTENSION OF
ISO/IEC 27017 · ISO/IEC 27018

PRIVACY INFORMATION MANAGEMENT SYSTEM
DNV
ISO/IEC 27701

BUSINESS CONTINUITY MANAGEMENT
DNV
ISO 22301

ISO27001:2022 – Annex A: Controls

Clause	Area	Objective	Applicable	Legal	Contract	Risk	Implemented
A.5	**Organizational Controls**						
A.5.1	Policies for information security	Information security 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	✓			Yes
A.5.2	Information security roles and responsibilities	Information security roles and responsibilities shall be defined and allocated according to the organization needs.	Yes			✓	Yes
A.5.3	Segregation of duties	Conflicting duties and conflicting areas of responsibility shall be segregated.	Yes			✓	Yes
A.5.4	Management responsibilities	Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.	Yes			✓	Yes
A.5.5	Contact with authorities	The organization shall establish and maintain contact with relevant authorities.	Yes	✓			Yes
A.5.6	Contact with special interest groups	The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.	Yes	✓			Yes
A.5.7	Threat Intelligence	Information relating to information security threats shall be collected and analysed to produce threat intelligence.	Yes	✓		✓	Yes
A.5.8	Information Security in project management	Information security shall be integrated into project management.	Yes			✓	Yes
A.5.9	Inventory of information and other associated assets	An inventory of information and other associated assets, including owners, shall be developed and maintained.	Yes			✓	Yes
A.5.10	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			✓	Yes
A.5.11	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			✓	Yes
A.5.12	Classification of Information	Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.	Yes	✓			Yes
A.5.13	Labelling of Information	An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	Yes			✓	Yes
A.5.14	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	✓	✓	✓	Yes
A.5.15	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 requirements.	Yes	✓		✓	Yes
A.5.16	Identity Management	The full life cycle of identities shall be managed.	Yes	✓			Yes
A.5.17	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	✓		✓	Yes
A.5.18	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	✓		✓	Yes
A.5.19	Information security in supplier relationships	Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier's products or services.	Yes			✓	Yes
A.5.20	Addressing security within supplier agreements	Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.	Yes	✓		✓	Yes
A.5.21	Managing information security in the information and communication technology (ICT) supply chain	Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain	Yes	✓		✓	Yes
A.5.22	Monitoring, review and change management of supplier services	The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.	Yes	✓		✓	Yes
A.5.23	Information security 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 requirements.	Yes	✓		✓	Yes

Clause	Area	Objective	Applicable	Legal	Contract	Risk	Implemented
A.5.24	Information security incident management planning and preparation	The organization shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.	Yes			✓	Yes
A.5.25	Assessment of and decision on information security events	The organization shall assess information security events and decide if they are to be categorized as information security incidents.	Yes	✓		✓	Yes
A.5.26	Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.	Yes	✓		✓	Yes
A.5.27	Learning from information security incidents	Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.	Yes			✓	Yes
A.5.28	Collection of evidence	The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.	Yes	✓		✓	Yes
A.5.29	Information security during disruption	The organization shall plan how to maintain information security at an appropriate level during disruption.	Yes	✓	✓	✓	Yes
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	✓	✓	✓	Yes
A.5.31	Legal, statutory, regulatory and contractual requirements	Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements shall be identified, documented and kept up to date.	Yes	✓		✓	Yes
A.5.32	Intellectual property rights	The organization shall implement appropriate procedures to protect intellectual property rights.	Yes	✓		✓	Yes
A.5.33	Protection of records	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release.	Yes	✓		✓	Yes
A.5.34	Privacy and protection of personally identifiable information	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	✓		✓	Yes
A.5.35	Independent review of information security	The organization's approach to managing information security and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant changes occur.	Yes	✓		✓	Yes
A.5.36	Compliance with policies, rules and standards for information security	Compliance with the organization's information security policy, topic-specific policies, rules and standards shall be regularly reviewed.	Yes	✓			Yes
A.5.37	Documented operating procedures	Operating procedures for information processing facilities shall be documented and made available to personnel who need them.	Yes			✓	Yes
A.6	**People Controls**						
A.6.1	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	✓			Yes
A.6.2	Terms and conditions of employment	The employment contractual agreements shall state the personnel's and the organization's responsibilities for information security.	Yes		✓	✓	Yes
A.6.3	Information security awareness and training	Personnel of the organization and relevant interested parties shall receive appropriate information security 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	✓		✓	Yes
A.6.4	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 policy violation.	Yes			✓	Yes
A.6.5	Responsibilities after termination or change of employment	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced and communicated to relevant personnel and other interested parties.	Yes		✓	✓	Yes
A.6.6	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	✓			Yes
A.6.7	Remote Working	Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.	Yes			✓	Yes

Clause	Area	Objective	Applicable	Legal	Contract	Risk	Implemented
A.6.8	Information security event reporting	The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	Yes	✓		✓	Yes
A.7	**Physical Controls**						
A.7.1	Physical Security perimeters	Security perimeters shall be defined and used to protect areas that contain information and other associated assets.	Yes	✓		✓	Yes
A.7.2	Physical entry	Secure areas shall be protected by appropriate entry controls and access points.	Yes			✓	Yes
A.7.3	Securing offices, rooms and facilities	Physical security for offices, rooms and facilities shall be designed and implemented.	Yes			✓	Yes
A.7.4	Physical security monitoring	Premises shall be continuously monitored for unauthorized physical access.	Yes			✓	Yes
A.7.5	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	✓		✓	Yes
A.7.6	Working in secure areas	Security measures for working in secure areas shall be designed and implemented.	Yes			✓	Yes
A.7.7	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			✓	Yes
A.7.8	Equipment siting and protection	Equipment shall be sited securely and protected.	Yes	✓		✓	Yes
A.7.9	Security of assets off-premises	Off-site assets shall be protected.	Yes			✓	Yes
A.7.10	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			✓	Yes
A.7.11	Supporting utilities	Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.	Yes			✓	Yes
A.7.12	Cabling security	Cables carrying power, data or supporting information services shall be protected from interception, interference or damage.	Yes			✓	Yes
A.7.13	Equipment maintenance	Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information.				✓	
A.7.14	Secure disposal or re-use 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			✓	Yes
A.8	**Technical Controls**						
A.8.1	User end point devices	Information stored on, processed by or accessible via user end point devices shall be protected.	Yes	✓		✓	Yes
A.8.2	Privileged access rights	The allocation and use of privileged access rights shall be restricted and managed.	Yes	✓		✓	Yes
A.8.3	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	✓		✓	Yes
A.8.4	Access to source code	Read and write access to source code, development tools and software libraries shall be appropriately managed.	Yes			✓	Yes
A.8.5	Secure authentication	Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control.	Yes	✓			Yes
A.8.6	Capacity management	The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.	Yes		✓	✓	Yes
A.8.7	Protection against malware	Protection against malware shall be implemented and supported by appropriate user awareness.	Yes			✓	Yes
A.8.8	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	✓		✓	Yes
A.8.9	Configuration management	Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed.	Yes			✓	Yes
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	✓	✓	✓	Yes
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-	Yes	✓		✓	Yes

Clause	Area	Objective	Applicable	Legal	Contract	Risk	Implemented
		specific policies, and business requirements, taking applicable legislation into consideration.					
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	✓			Yes
A.8.13	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			✓	Yes
A.8.14	Redundancy of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	Yes	✓	✓	✓	Yes
A.8.15	Logging	Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed.	Yes	✓		✓	Yes
A.8.16	Monitoring activities	Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.	Yes			✓	Yes
A.8.17	Clock synchronization	The clocks of information processing systems used by the organization shall be synchronized to approved time sources.	Yes	✓		✓	Yes
A.8.18	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	✓		✓	Yes
A.8.19	Installation of software on operational systems	Procedures and measures shall be implemented to securely manage software installation on operational systems.	Yes	✓		✓	Yes
A.8.20	Networks security	Networks and network devices shall be secured, managed and controlled to protect information in systems and applications.	Yes			✓	Yes
A.8.21	Security of network services	Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored.	Yes			✓	Yes
A.8.22	Segregation of networks	Groups of information services, users and information systems shall be segregated in the organization’s networks.	Yes	✓		✓	Yes
A.8.23	Web filtering	Access to external websites shall be managed to reduce exposure to malicious content.	Yes			✓	Yes
A.8.24	Use of cryptography	Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented.	Yes	✓			Yes
A.8.25	Secure development life cycle	Rules for the secure development of software and systems shall be established and applied.	Yes			✓	Yes
A.8.26	Application security requirements	Information security requirements shall be identified, specified and approved when developing or acquiring applications.	Yes			✓	Yes
A.8.27	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			✓	Yes
A.8.28	Secure coding	Secure coding principles shall be applied to software development.	Yes			✓	Yes
A.8.29	Security testing in development and acceptance	Security testing processes shall be defined and implemented in the development life cycle.	Yes			✓	Yes
A.8.30	Outsourced development	The organization shall direct, monitor and review the activities related to outsourced system development.	Yes			✓	Yes
A.8.31	Separation of development, test and production environments	Development, testing and production environments shall be separated and secured.	Yes			✓	Yes
A.8.32	Change management	Changes to information processing facilities and information systems shall be subject to change management procedures.	Yes			✓	Yes
A.8.33	Test information	Test information shall be appropriately selected, protected and managed.	Yes	✓		✓	Yes
A.8.34	Protection of information security 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	✓		✓	Yes

ISO27017:2015 – Annex A (Requirements for Cloud Service Customers)

Clause	Area	Objective	Applicable	Legal	Contract	Risk	Implemented
CLD.6.3	**Relationship between cloud service customer and cloud service provider**	**Objective:** To clarify the relationship regarding shared roles and responsibilities between the cloud service customer and the cloud service provider for information security management.					
CLD.6.3.1	Shared roles and responsibilities within a cloud computing environment	Responsibilities for shared information security roles in the use of the cloud service should be allocated to identified parties, documented, communicated and implemented by both the cloud service customer and the cloud service provider.	Yes	✓			Yes
CLD.8.1	**Responsibility for assets**	The objective specified in clause 8.1 of ISO/IEC 27002 applies.	Yes				
CLD.8.1.5	Removal of cloud service customer assets	Assets of the cloud service customer that are on the cloud service provider's premises should be removed, and returned if necessary, in a timely manner upon termination of the cloud service agreement.	Yes	✓			Yes
CLD.9.5	**Access control of cloud service customer data in shared virtual environment**	**Objective:** To mitigate information security risks when using the shared virtual environment of cloud computing.					
CLD.9.5.1	Segregation in virtual computing environments	A cloud service customer's virtual environment running on a cloud service should be protected from other cloud service customers and unauthorized persons.	Yes			✓	Yes
CLD.9.5.2	Virtual machine hardening	Virtual machines in a cloud computing environment should be hardened to meet business needs.	Yes	✓		✓	Yes
CLD.12.1	**Operational procedures and responsibilities**	The objective specified in clause 12.1 of ISO/IEC 27002 applies.		✓		✓	
CLD.12.1.5	Administrator's operational security	Procedures for administrative operations of a cloud computing environment should be defined, documented and monitored.	Yes	✓		✓	Yes
CLD.12.4	**Logging and monitoring**	The objective specified in clause 12.4 of ISO/IEC 27002 applies.		✓		✓	
CLD.12.4.5	Monitoring of Cloud Services	The cloud service customer should have the capability to monitor specified aspects of the operation of the cloud services that the cloud service customer uses.	Yes	✓		✓	Yes
CLD.13.1	**Network security management**	The objective specified in clause 13.1 of ISO/IEC 27002 applies.					
CLD.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 should be verified based on the cloud service provider's network security policy.	No	Cloud Service provider does not have network security policy			N/A

ISO27018:2019 – Annex A (Extended control set for PII Protection)

Clause	Area	Objective	Applicable	Legal	Contract	Risk	Implemented
A.2	**Consent and Choice**						
A.2.1	Obligation to co-operate regarding PII principals' rights	The public cloud PII processor should provide the cloud service customer with the means to enable them to fulfil their obligation to facilitate the exercise of PII principals' rights to access, correct and/or erase PII pertaining to them.	Yes	✓			Yes
A.3	**Purpose legitimacy and specification**						
A.3.1	Public cloud PII processor's purpose	PII to be processed under a contract should not be processed for any purpose independent of the instructions of the cloud service customer.	Yes	✓	✓		Yes
A.3.2	Public cloud PII processor's commercial use	PII processed under a contract should not be used by the public cloud PII processor for the purposes of marketing and advertising without express consent. Such consent should not be a condition of receiving the service. NOTE This control is an addition to the more general control in A.3.1 and does not replace or otherwise supersede it.	Yes	✓	✓		Yes
A.4	**Collection limitation**	No additional controls are relevant to this privacy principle.					
A.5	**Data minimization**						
A.5.1	Secure erasure of temporary files	Temporary files and documents should be erased or destroyed within a specified, documented period.	Yes			✓	Yes
A.6	**Use, retention, and disclosure limitation**						
A.6.1	PII disclosure information	The contract between the public cloud PII processor and the cloud service customer should require the public cloud PII 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 PII by a law enforcement authority, unless such a disclosure is otherwise prohibited.	Yes		✓		Yes
A.6.2	Recording of PII disclosures	Disclosures of PII to third parties should be recorded, including what PII has been disclosed, to whom and at what time.	Yes		✓		Yes
A.7	**Accuracy and quality**	No additional controls are relevant to this privacy principle.					
A.8	**Openness, transparency and notice**						
A.8.1	Disclosure of sub-contracted PII processing	The use of sub-contractors by the public cloud PII processor to process PII should be disclosed to the relevant cloud service customers before their use.	Yes		✓		Yes
A.9	**Individual participation and access**	No additional controls are relevant to this privacy principle.					
A.10	**Accountability**						
A.10.1	Notification of a data breach involving PII	The public cloud PII processor should promptly notify the relevant cloud service customer in the event of any unauthorized access to PII or unauthorized access to processing equipment or facilities resulting in loss, disclosure or alteration of PII.	Yes	✓	✓		Yes
A.10.2	Retention period for administrative security policies and guidelines	Copies of security policies and operating procedures should be retained for a specified, documented period on replacement (including updating).	Yes	✓			Yes
A.10.3	PII return, transfer and disposal	The public cloud PII processor should have a policy in respect of the return, transfer and/or disposal of PII and should make this policy available to the cloud service customer.	Yes		✓		Yes
A.11	**Information security**						
A.11.1	Confidentiality or non-disclosure agreements	Individuals under the public cloud PII processor's control with access to PII should be subject to a confidentiality obligation.	Yes		✓		Yes
A.11.2	Restriction of the creation of hardcopy material	The creation of hardcopy material displaying PII should be restricted.	Yes			✓	Yes
A.11.3	Control and logging of data restoration	There should be a procedure for, and a log of, data restoration efforts.	Yes			✓	Yes
A.11.4	Protecting data on storage media leaving the premises	PII on media leaving the organization's premises should be subject to an authorization procedure and should not be accessible to anyone other than authorized personnel (e.g. by encrypting the data concerned).	Yes			✓	Yex
A.11.5	Use of unencrypted portable storage media and devices	Portable physical media and portable devices that do not permit encryption should not be used except where it is unavoidable, and any use of such portable media and devices should be documented.	Yes			✓	Yes

Clause	Area	Objective	Applicable	Legal	Contract	Risk	Implemented
A.11.6	Encryption of PII transmitted over public data-transmission networks	PII that is transmitted over public data-transmission networks should be encrypted prior to transmission.	Yes	✓		✓	Yes
A.11.7	Secure disposal of hardcopy materials	Where hardcopy materials are destroyed, they should be destroyed securely using mechanisms such as cross-cutting, shredding, incinerating, pulping, etc.	Yes	✓		✓	Yes
A.11.8	Unique use of user IDs	If more than one individual has access to stored PII, then they should each have a distinct user ID for identification, authentication and authorization purposes.	Yes	✓		✓	Yes
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 should be maintained.	Yes	✓		✓	Yes
A.11.10	User ID management	De-activated or expired user IDs should not be granted to other individuals.	Yes	✓		✓	Yes
A.11.11	Contract measures	Contracts between the cloud service customer and the public cloud PII processor should 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 should not be subject to unilateral reduction by the public cloud PII processor.	Yes	✓	✓		Yes
A.11.12	Sub-contracted PII processing	Contracts between the public cloud PII processor and any sub-contractors that process PII should specify minimum technical and organizational measures that meet the information security and PII protection obligations of the public cloud PII processor. Such measures should not be subject to unilateral reduction by the sub-contractor.	Yes		✓		Yes
A.11.13	Access to data on pre-used data storage space	The public cloud PII processor should ensure 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.	Yes			✓	Yes
A.12	**Privacy compliance**						
A.12.1	Geographical location of PII	The public cloud PII processor should specify and document the countries in which PII can possibly be stored.	Yes	✓		✓	Yes
A.12.2	Intended destination of PII	PII transmitted using a data-transmission network should be subject to appropriate controls designed to ensure that data reaches its intended destination.	Yes			✓	Yes

ISO27701:2019 – Annex A (Additional requirements for controllers)

Clause	Area	Objective	Applicable	Legal	Contract	Risk	Implemented
A.7							
A.7.2	**Conditions for collection and processing**	**Objective:** To determine and document that processing is lawful, with legal basis as per applicable jurisdictions, and with clearly defined and legitimate purposes.					
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	✓	✓		Yes
A.7.2.2	Identify lawful basis	The organization shall determine, document and comply with the relevant lawful basis for the processing of PII for the identified purposes.	Yes	✓	✓		Yes
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	✓			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	✓			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	✓		✓	Yes
A.7.2.6	Contracts with PII processors	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.	Yes	✓	✓		Yes
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.	No	DDY is not joint controller			No
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	✓			Yes
A.7.3	**Obligations to PII principals**	**Objective:** To ensure that PII principals are provided with appropriate information about the processing of their PII and to meet any other applicable obligations to PII principals related to the processing of their PII.					
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 their PII and provide the means to meet these obligations.	Yes	✓			Yes
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	✓			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	✓			Yes
A.7.3.4	Providing mechanism to modify or with-draw consent	The organization shall provide a mechanism for PII principals to modify or withdraw their consent.	Yes	✓			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, procedures and/or mechanisms to meet their obligations to PII principals to access, correct and/or erase their PII.	Yes	✓			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, procedures and/or mechanisms to do so.	No	DDY does not use third parties that need to be informed			No
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	✓			Yes
A.7.3.9	Handling requests	The organization shall define and document policies and procedures for handling and responding to legitimate requests from PII principals.	Yes	✓			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	✓			Yes
A.7.4	**Privacy by design and privacy by default**	**Objective:** To ensure that processes and systems are designed such that the collection and processing (including use, disclosure, retention, transmission and disposal) are limited to what is necessary for the identified purpose.					

Clause	Area	Objective	Applicable	Legal	Contract	Risk	Implemented
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	✓			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	✓			Yes
A.7.4.3	Accuracy and quality	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.	Yes	✓		✓	Yes
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	✓		✓	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	✓			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 procedures within a specified, documented period.	Yes	✓		✓	Yes
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	✓			Yes
A.7.4.8	Disposal	The organization shall have documented policies, procedures and/or mechanisms for the disposal of PII.	Yes	✓			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	✓			Yes
A.7.5	**PII sharing, transfer and disclosure**	**Objective:** To determine whether and document when PII is shared, transferred to other jurisdictions or third parties and/or disclosed in accordance with applicable obligations.					
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	✓			Yes
A.7.5.2	Countries and inter-national 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	✓			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	✓			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	✓			Yes

ISO27701:2019 – Annex B (Additional requirements for processors)

Clause	Area	Objective	Applicable	Legal	Contract	Risk	Implemented
B.8.2	**Conditions for collection and processing**	**Objective:** To determine and document that processing is lawful, with legal basis as per applicable jurisdictions, and with clearly defined and legitimate purposes.					
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	✓	✓		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 purpose expressed in the documented instructions of the customer.	Yes	✓	✓		Yes
B.8.2.3	Marketing and advertising use	The organization shall not use PII processed under a contract for the purpose of marketing and advertising without establishing that prior consent was obtained from the appropriate PII principal. The organisation shall not make providing such consent a condition for receiving the service.	Yes	✓	✓		Yes
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	✓	✓		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	✓	✓		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 the PII carried out on behalf of a customer.	Yes	✓			Yes
B.8.3	**Obligations to PII principals**	**Objective:** To ensure that PII principals are provided with the appropriate information about the processing of their PII, and to meet any other applicable obligations to PII principals related to the processing of their PII.					
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	✓			Yes
B.8.4	**Privacy by design and privacy by default**	**Objective:** To ensure that processes and systems are designed such that the collection and processing of PII (including use, disclosure, retention, transmission and disposal) are limited to what is necessary for the identified purpose.					
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.	Yes	✓			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	✓			Yes
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.	Yes	✓			Yes
B.8.5	**PII sharing, transfer and disclosure**	**Objective:** To determine whether and document when PII is shared, transferred to other jurisdictions or third parties and/or disclosed in accordance with applicable obligations.					
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	✓			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	✓			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	✓			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	✓			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	✓	✓		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	✓			Yes

Clause	Area	Objective	Applicable	Legal	Contract	Risk	Implemented
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	✓			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	✓	✓		Yes