SoA (Statement of Applicability)

Revision 6 - May 10, 2025

Publication summary

Created by:	Alessandro Gai (CISO) & Eliza Bounouar (DPO)
Classification:	**PUBLIC**

Change/revision history

Date	Rev.	By	Description of change
Nov 01, 2023	0	Alessandro Gai	Initial draft
Jan 17, 2024	1	Alessandro Gai	Final draft
Jul 20, 2024	2	Alessandro Gai	Addedd DORA and NIS2
Sep 06, 2024	3	Alessandro Gai	New template
Feb 11, 2025	4	Alessandro Gai	Extracted Internal Audit
Mar 07, 2025	5	Alessandro Gai & Eliza Bounouar	27701 controls
May 10, 2025	6	Alessandro Gai	Exclusion of 7.04 and 7.12

Term of validity

This version replaces all previous versions and is valid until the next version is issued or the expiration date if it has been set.

Distribution list

N/A

Reference documents

N/A

ISO27002:22 Controls			Inclusion[1]		Justification	Implemented
5.00	**Organizational controls**					
5.01	**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	REG	Required to comply with legal, regulatory, and certification requirements like ISO 27001.	Yes
5.02	**Information security roles and responsibilities**	Information security roles and responsibilities shall be defined and allocated according to the organization needs.	Yes	BP	Ensures clear accountability and responsibility for information security within the organization.	Yes
5.03	**Segregation of duties**	Conflicting duties and conflicting areas of responsibility shall be segregated.	Yes	RA	Prevents conflicts of interest and reduces risk of fraud or accidental security breaches.	Yes
5.04	**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	BP	Ensures leadership commitment to information security policies and procedures.	Yes

[1] REG: The control is related to a regulatory or certification requirement
CON: The control is required due to a contractual obligation
BP: The control is needed according to best practices
RA: The control is needed to mitigate inherent risk to control objectives

ISO27002:22 Controls			Inclusion[1]		Justification	Implemented
5.05	**Contact with authorities**	The organization shall establish and maintain contact with relevant authorities.	Yes	REG	Necessary for regulatory compliance and incident response coordination.	Yes
5.06	**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	BP	Helps stay informed about security threats and best practices.	Yes
5.07	**Threat intelligence**	Information relating to information security threats shall be collected and analyzed to produce threat intelligence.	Yes	RA	To proactively monitor and respond to emerging cyber threats such as ransomware, social engineering, AI-powered cyberattacks, and faster exploitation of vulnerabilities.	Yes
5.08	**Information security in project management**	Information security shall be integrated into project management.	Yes	RA	Ensures security is integrated into the development and implementation of projects.	Yes
5.09	**Inventory of information and other associated assets**	An inventory of information and other associated assets, including owners, shall be developed and maintained.	Yes	RA	To ensure that sensitive data, including customer and personal data, is properly identified and protected against breaches, leaks, and manipulation.	Yes
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	RA	To prevent misuse of company assets that could lead to security incidents, such as unauthorized cloud usage or improper handling of confidential information.	Yes

ISO27002:22 Controls			Inclusion[1]		Justification	Implemented
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	CON	Required to ensure company data and assets are returned when employees or contractors leave.	Yes
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	BP	Protects sensitive data based on confidentiality, integrity, and availability needs.	Yes
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	BP	Supports effective classification and handling of information assets.	Yes
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	REG	Ensures secure transmission of sensitive data as per compliance standards.	Yes
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	RA	Reduces the risk of unauthorized access to sensitive data and systems.	Yes
5.16	**Identity management**	The full life cycle of identities shall be managed.	Yes	RA	Ensures proper lifecycle management of user identities and access.	Yes

ISO27002:22 Controls			Inclusion[1]		Justification	Implemented
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	RA	Enhances security by enforcing strong authentication and credential management.	Yes
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	RA	Ensures contractual compliance regarding access restrictions for third parties and employees.	Yes
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	CON	Manages risks from suppliers and third-party vendors handling company data.	Yes
5.20	**Addressing information security within supplier agreements**	Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.	Yes	CON	Ensures contractual security obligations are met by suppliers.	Yes
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	RA	Enhances security of software and service dependencies in cloud environments.	Yes
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	BP	Ensures suppliers continue meeting security requirements.	Yes

ISO27002:22 Controls			Inclusion[1]		Justification	Implemented
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	REG	Critical for securing cloud environments and meeting regulatory obligations such as GDPR.	Yes
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	REG	Required for compliance with regulatory frameworks and certifications.	Yes
5.25	**Assessment 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	CON	Ensures events are analyzed and classified correctly to mitigate risks.	Yes
5.26	**Response to information security incidents**	Information security incidents shall be responded to in accordance with the documented procedures.	Yes	CON	Meets contractual obligations with incident response.	Yes
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	BP	Improves security posture by learning from past incidents.	Yes
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	BP	Ensures forensic integrity and legal compliance in case of security breaches.	Yes

ISO27002:22 Controls			Inclusion[1]		Justification	Implemented
5.29	**Information security during disruption**	The organization shall plan how to maintain information security at an appropriate level during disruption.	Yes	BP	Ensures continued security operations during incidents or crises.	Yes
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	CON	Meets contractual obligations for service availability and continuity.	Yes
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	REG	Ensures compliance with legal and contractual obligations.	Yes
5.32	**Intellectual property rights**	The organization shall implement appropriate procedures to protect intellectual property rights.	Yes	REG	Protects software and data against unauthorized use and breaches.	Yes
5.33	**Protection of records**	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release.	Yes	RA	Ensures integrity and availability of business-critical information.	Yes
5.34	**Privacy and protection of personal identifiable information (PII)**	The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable	Yes	REG	Ensures compliance with data privacy regulations like GDPR.	Yes

ISO27002:22 Controls			Inclusion[1]		Justification	Implemented
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	BP	Provides assurance that security measures are effective.	Yes
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	RA	Reduces risks by ensuring policy adherence across the company.	Yes
5.37	**Documented operating procedures**	Operating procedures for information processing facilities shall be documented and made available to personnel who need them.	Yes	BP	Ensures consistency and reliability in security operations.	Yes
6.00	**People controls**					
6.01	**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	RA	Reduces risk of insider threats (at least for critical roles).	Yes
6.02	**Terms and conditions of employment**	The employment contractual agreements shall state the personnel's and the organization's responsibilities for information security.	Yes	CON	Contractual obligations include security responsibilities.	Yes
6.03	**Information security awareness, education 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	RA	Ensures employees understand security best practices.	Yes

ISO27002:22 Controls			Inclusion[1]		Justification	Implemented
6.04	**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	RA	Prevents policy violations through enforcement mechanisms.	Yes
6.05	**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	CON	Defined in employment contracts.	Yes
6.06	**Confidentiality or non- disclosure agreements**	Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information should be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.	Yes	CON	Required for data protection and IP security.	Yes
6.07	**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	RA	Addresses security risks in remote environments.	Yes
6.08	**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	BP	Encourages a proactive security culture.	Yes
7.00	**Physical controls**					
7.01	**Physical security perimeters**	Security perimeters shall be defined and used to protect areas that contain information and other associated assets.	Yes	BP	Ensures controlled access and prevent unauthorized access to sensitive areas where data is processed or stored. (This is also enforced through contractual agreements with our cloud providers)	Yes

ISO27002:22 Controls			Inclusion[1]		Justification	Implemented
7.02	**Physical entry**	Secure areas should be protected by appropriate entry controls and access points.	Yes	BP	Prevents unauthorized access to facilities.	Yes
7.03	**Securing offices, rooms and facilities**	Physical security for offices, rooms and facilities shall be designed and implemented.	Yes	BP	Reduces risk of physical breaches.	Yes
7.04	**Physical security monitoring**	Premises should be continuously monitored for unauthorized physical access.	No		Sensitive information assets and the majority of non-sensitive information assets are not hosted in our offices but with our cloud providers. Based on the results of our risk assessment, we believe that the other physical measures in place are sufficient to cover the level of risk for our office locations.	No
7.05	**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 should be designed and implemented.	Yes	BP	Mitigates risks from natural disasters or attacks. (This is also enforced through contractual agreements with our cloud providers)	Yes
7.06	**Working in secure areas**	To protect information and other associated assets in secure areas from damage and unauthorized interference by personnel working in these areas.	Yes	BP	Protects confidential operations from exposure.	Yes
7.07	**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	BP	Prevents unauthorized access to sensitive data.	Yes

ISO27002:22 Controls			Inclusion[1]		Justification	Implemented
7.08	**Equipment siting and protection**	Equipment shall be sited securely and protected.	Yes	BP	Ensures secure placement of critical IT assets.	Yes
7.09	**Security of assets off- premises**	Off-site assets shall be protected.	Yes	BP	Protects remote work assets.	Yes
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	BP	Prevents unauthorized data access.	Yes
7.11	**Supporting utilities**	Information processing facilities should be protected from power failures and other disruptions caused by failures in supporting utilities.	Yes	BP	Ensures power and connectivity continuity.	Yes
7.12	**Cabling security**	Cables carrying power, data or supporting information services should be protected from interception, interference, or damage.	No		efficy primarily uses wireless networks and based on risk assessment result we believe that risk associated with unsecured cabling are negligible.	No
7.13	**Equipment maintenance**	Equipment should be maintained correctly to ensure availability, integrity and confidentiality of information.	Yes	BP	Ensures continuous operation of IT systems.	Yes

ISO27002:22 Controls			Inclusion[1]		Justification	Implemented
7.14	**Secure disposal or re-use of equipment**	Items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	Yes	BP	Prevents data leakage through hardware disposal.	Yes
8.00	**Technological controls**					
8.01	**User end point devices**	Information stored on, processed by or accessible via user endpoint devices should be protected.	Yes	RA	To prevent malware infections, ransomware, and unauthorized access to sensitive systems via compromised endpoints.	Yes
8.02	**Privileged access rights**	The allocation and use of privileged access rights should be restricted and managed.	Yes	RA	To mitigate the risk of misuse of privileged access, ensuring only authorized personnel can perform critical actions.	Yes
8.03	**Information access restriction**	Access to information and other associated assets should be restricted in accordance with the established topic-specific policy on access control.	Yes	RA	To control access to sensitive information, reducing the risk of data breaches and unauthorized access.	Yes
8.04	**Access to source code**	Read and write access to source code, development tools and software libraries should be appropriately managed.	Yes	BP	To protect our code confidentiality and prevent unauthorized modifications to the source code.	Yes
8.05	**Secure authentication**	Secure authentication technologies and procedures should be implemented based on information access restrictions and the topic-specific policy on access control.	Yes	RA	To ensure robust authentication mechanisms are in place, reducing the risk of unauthorized access.	Yes

ISO27002:22 Controls			Inclusion[1]		Justification	Implemented
8.06	**Capacity management**	The use of resources should be monitored and adjusted in line with current and expected capacity requirements.	Yes	BP	To ensure that our resources are used efficiently and can handle current and future demands.	Yes
8.07	**Protection against malware**	Protection against malware should be implemented and supported by appropriate user awareness.	Yes	RA	To prevent malware infections that could compromise the integrity and availability of information systems.	Yes
8.08	**Management of technical vulnerabilities**	Information about technical vulnerabilities of information systems in use should be obtained, the organization's exposure to such vulnerabilities should be evaluated and appropriate measures should be taken.	Yes	RA	To identify and mitigate vulnerabilities in a timely manner, reducing the risk of exploitation.	Yes
8.09	**Configuration management**	Information about technical vulnerabilities of information systems in use should be obtained, the organization's exposure to such vulnerabilities should be evaluated and appropriate measures should be taken.	Yes	RA	To ensure that systems are configured securely and consistently, reducing the risk of misconfigurations.	Yes
8.10	**Information deletion**	Configurations, including security configurations, of hardware, software, services and networks should be established, documented, implemented, monitored and reviewed.	Yes	REG	To comply with data protection regulations, ensuring that information is securely deleted when no longer needed.	Yes
8.11	**Data masking**	Information stored in information systems, devices or in any other storage media should be deleted when no longer required.	Yes	RA	To protect sensitive data by masking it, reducing the risk of exposure during processing and testing.	Yes

ISO27002:22 Controls			Inclusion[1]		Justification	Implemented
8.12	**Data leakage prevention**	Data leakage prevention measures should be applied to systems, networks and any other devices that process, store or transmit sensitive information.	Yes	RA	To prevent unauthorized transfer of sensitive information outside the organization.	Yes
8.13	**Information backup**	Backup copies of information, software and systems should be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.	Yes	CON	To ensure data availability and integrity in case of data loss or corruption.	Yes
8.14	**Redundancy of information processing facilities**	Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.	Yes	CON	To ensure business continuity by having redundant systems in place.	Yes
8.15	**Logging**	Logs that record activities, exceptions, faults and other relevant events should be produced, stored, protected and analysed.	Yes	BP	To maintain an audit trail of activities, aiding in incident detection and response.	Yes
8.16	**Monitoring activities**	Networks, systems and applications should be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.	Yes	RA	To detect and respond to security incidents in a timely manner.	Yes
8.17	**Clock synchronization**	The clocks of information processing systems used by the organization should be synchronized to approved time sources.	Yes	BP	To ensure accurate timestamps in logs, aiding in incident investigation and correlation.	Yes

ISO27002:22 Controls			Inclusion[1]		Justification	Implemented
8.18	**Use of privileged utility programs**	The use of utility programs that can be capable of overriding system and application controls should be restricted and tightly controlled.	Yes	RA	To control the use of powerful utility programs, reducing the risk of misuse.	Yes
8.19	**Installation of software on operational systems**	Procedures and measures should be implemented to securely manage software installation on operational systems.	Yes	RA	To ensure that only authorized and tested software is installed, reducing the risk of introducing vulnerabilities.	Yes
8.20	**Networks security**	Networks and network devices should be secured, managed and controlled to protect information in systems and applications.	Yes	BP	To protect the network infrastructure from unauthorized access and attacks.	Yes
8.21	**Security of network services**	Security mechanisms, service levels and service requirements of network services should be identified, implemented and monitored.	Yes	BP	To ensure that network services are secure and available.	Yes
8.22	**Segregation of networks**	Groups of information services, users and information systems should be segregated in the organization’s networks.	Yes	RA	To reduce the risk of unauthorized access and limit the impact of security incidents.	Yes
8.23	**Web filtering**	Access to external websites should be managed to reduce exposure to malicious content.	Yes	BP	To prevent access to malicious or inappropriate websites, reducing the risk of malware infections.	Yes

ISO27002:22 Controls			Inclusion[1]		Justification	Implemented
8.24	**Use of cryptography**	Rules for the effective use of cryptography, including cryptographic key management, should be defined and implemented.	Yes	REG	To comply with data protection regulations and protect sensitive information during transmission and storage.	Yes
8.25	**Secure development life cycle**	Rules for the secure development of software and systems should be established and applied.	Yes	RA	To ensure that security is integrated into the development process, reducing the risk of vulnerabilities in software.	Yes
8.26	**Application security requirements**	Information security requirements should be identified, specified and approved when developing or acquiring applications.	Yes	RA	To define and implement security requirements for applications, ensuring they are secure by design.	Yes
8.27	**Secure system architecture and engineering principles**	Principles for engineering secure systems to be established, documented, maintained and applied to any information system development activities.	Yes	BP	To ensure that systems are designed and built with security in mind, reducing the risk of vulnerabilities.	Yes
8.28	**Secure coding**	Secure coding principles should be applied to software development.	Yes	RA	To ensure that code is written securely, reducing the risk of vulnerabilities.	Yes
8.29	**Security testing in development and acceptance**	Security testing processes should be defined and implemented in the development life cycle.	Yes	RA	To identify and fix security issues before software is deployed, reducing the risk of vulnerabilities.	Yes

ISO27002:22 Controls			Inclusion[1]		Justification	Implemented
8.30	**Outsourced development**	The organization should direct, monitor and review the activities related to outsourced system development.	Yes	BP	To ensure that security requirements are met by third-party developers, reducing the risk of vulnerabilities.	Yes
8.31	**Separation of development, test and production environments**	Development, testing and production environments should be separated and secured.	Yes	RA	To prevent unauthorized access and changes to production systems, reducing the risk of incidents.	Yes
8.32	**Change management**	Changes to information processing facilities and information systems should be subject to change management procedures.	Yes	BP	To ensure that changes are controlled and tested, reducing the risk of introducing vulnerabilities.	Yes
8.33	**Test information**	Test information should be appropriately selected, protected and managed.	Yes	BP	To protect sensitive information used in testing, reducing the risk of data breaches.	Yes
8.34	**Protection of information systems during audit testing**	Audit tests and other assurance activities involving assessment of operational systems should be planned and agreed between the tester and appropriate management.	Yes	BP	To ensure that audit activities do not compromise the security or availability of information systems.	Yes

ISO27701:19 Controls			Inclusion[1]		Justification	Implemented
Controller A.7.2.1	**Identify and document purpose**	The organization should identify and document the specific purposes for which the PII will be processed	Yes	REG	efficy processes personal data as a controller and must therefore have a purpose for the processing of perosnal data	Yes
Controller A.7.2.2	**Identify lawful basis**	The organization should determine, document and comply with the relevant lawful basis for the processing of PII for the identified purposes	Yes	REG	efficy processes personal data as a controller and must therefore have a lawful basis for the processing of perosnal data	Yes
Controller A.7.2.3	**Determining when and how consent is to be obtained**	The organization should 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	REG	DPO is involved when necessary to ensure that the consent obtained is valid. In efficy's activities consent is mainly collected for marketing purposes and recorded in the Apsis One platform	Yes
Controller A.7.2.4	**Obtain and record consent**	The organization should obtain and record consent from PII principals according to the documented processes	Yes	REG	In efficy's activities consent is mainly collected for marketing purposes and recorded in the Apsis One platform	Yes
Controller A.7.2.5	**Privacy Impact Assessment**	The organization should 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	REG	PIA performed when activities identified have a risk to impact data subjects' rights and freedoms	Yes
Controller A.7.2.6	**Contracts with PII processors**	The organization should have a written contract with any PII processor that it uses, and should ensure that their contracts with PII processors address the implementation of the appropriate controls in Annex B	Yes	CON	DPA are always signed when processing personal data. When contracting with sub-processors, efficy ensures that the obligations undertaken are also reported in the subsequent DPA	Yes

ISO27701:19 Controls			Inclusion[1]		Justification	Implemented
Controller A.7.2.7	**Joint PII controller**	The organization should determine respective roles and responsibilities for the processing of PII (including PII protection and security requirements) with any joint PII controller	Yes	REG	efficy group companies are joint controllers for the processing of employee personal data.	Yes
Controller A.7.2.8	**Records related to processing of PII**	The organization should determine and securely maintain the necessary records in support of its obligations for the processing of PII	Yes	REG	A record of processing activities is maintained by efficy to ensure the processing of personal data in accordance with the applicable regulation.	Yes
Controller A.7.3.1	**Determining and fulfilling obligations to PII principals**	The organization should 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	REG	Processes are in place to ensure that data subjects can exercise their rights.	Yes
Controller A.7.3.2	**Determining information for PII principals**	The organization should 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	REG	DPO involved when new processing operations are carried out to ensure that the appropriate information is delivered.	Yes
Controller A.7.3.3	**Providing information to PII principals**	The organization should provide PII principals with clear and easily accessible information identifying the PII controller and describing the processing of their PII	Yes	REG	Information done at the collection of the data, through privacy policies covering all the processing activities	Yes
Controller A.7.3.4	**Providing mechanism to modify or withdraw consent**	The organization should provide a mechanism for PII principals to modify or withdraw their consent	Yes	CON	When relying on consent, Efficy records consent and allows data subjects to withdraw their consent easily (unsubcription link, extranet etc..)	Yes

ISO27701:19 Controls			Inclusion[1]		Justification	Implemented
Controller A.7.3.5	**Providing mechanism to object to PII processing**	The organization should provide a mechanism for PII principals to object to the processing of their PII	Yes	REG	Where applicable objection from the data subjects to the processing of their information is recorded	Yes
Controller A.7.3.6	**Access, correction and/or erasure**	The organization should implement policies, procedures and/or mechanisms to meet their obligations to PII principals to access, correct and/or erase their PII	Yes	REG	When processinhg personal daya, efficy needs to ensure that the data is accurate and up to date, and therefore allows data subject to correct their data. Access and deletion requests are also handled according to the applicable laws and regulations.	Yes
Controller A.7.3.7	**PII controllers' obligations to inform third parties**	The organization should 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	Yes	REG	When data is shared with third parties, such sharing is recorded in the record of processing activities and data subjects must be informed.	Yes
Controller A.7.3.8	**Providing copy of PII processed**	The organization should be able to provide a copy of the PII that is processed when requested by the PII principal	Yes	REG	Procedure to handle data subject requests defined, easy tools to use implemented to facilitate such requests.	Yes
Controller A.7.3.9	**Handling requests**	The organization should define and document policies and procedures for handling and responding to legitimate requests from PII principals	Yes	REG	Policy defined and implemented to ensure correct handling of data subjects requests	Yes
Controller A.7.3.10	**Automated decision making**	The organization should 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	No		No automated decision making processes are implemented	No

ISO27701:19 Controls			Inclusion[1]		Justification	Implemented
Controller A.7.4.1	**Limit collection**	The organization should limit the collection of PII to the minimum that is relevant, proportional and necessary for the identified purposes	Yes	BP	Privacy by design policy defined and implemented	Yes
Controller A.7.4.2	**Limit processing**	The organization should limit the processing of PII to that which is adequate, relevant and necessary for the identified purposes	Yes	BP	Privacy by design policy defined and implemented	Yes
Controller A.7.4.3	**Accuracy and quality**	The organization should 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	REG	When processinhg personal daya, efficy needs to ensure that the data is accurate and up to date, and therefore allows data subject to correct their data.	Yes
Controller A.7.4.4	**PII minimization objectives**	The organization should define and document data minimization objectives and what mechanisms (such as de-identification) are used to meet those objectives	Yes	BP	Privacy by design policy defined and implemented	Yes
Controller A.7.4.5	**PII de-identification and deletion at the end of processing**	The organization should 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	REG	efficy has defined data retention periods to ensure that no personal data is stored longer than necessary.	Yes
Controller A.7.4.6	**Temporary files**	The organization should ensure that temporary files created as a result of the processing of PII are disposed of (e.g. erased or destroyed) following documented procedures within a specified, documented period	Yes	CON	Procedures implemented regarding the deletion of data and backup of data	Yes

ISO27701:19 Controls			Inclusion[1]		Justification	Implemented
Controller A.7.4.7	**Retention**	The organization should not retain PII for longer than is necessary for the purposes for which the PII is processed	Yes	BP	efficy has defined data retention periods to ensure that no personal data is stored longer than necessary.	Yes
Controller A.7.4.8	**Disposal**	The organization should have documented policies, procedures and/or mechanisms for the disposal of PII	Yes	CON	efficy has defined a device policy containing undertakings regarding the disposabl of IT devices containing personal data	Yes
Controller A.7.4.9	**PII transmission controls**	The organization should 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	REG	efficy must transfer PII in a secure way, which is ensured through the implementation of technical solutions and role based access	Yes
Controller A.7.5.1	**Identify basis for PII transfer between jurisdictions**	The organization should identify and document the relevant basis for transfers of PII between jurisdictions	Yes	REG	Relevant transfer basis identified in the record of processing activities	Yes
Controller A.7.5.2	**Countries and international organizations to which PII can be transferred**	The organization should specify and document the countries and international organizations to which PII can possibly be transferred	Yes	CON	efficy has defined such requirements in the privacfy by design policy.	Yes
Controller A.7.5.3	**Records of transfer of PII**	The organization should 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	REG	Transfer and sharing of personal data to third parties are recorded in the record of processing activities and in the logs of the respective applications.	Yes

ISO27701:19 Controls			Inclusion[1]		Justification	Implemented
Controller A.7.5.4	**Records of PII disclosure to third parties**	The organization should record disclosures of PII to third parties, including what PII has been disclosed, to whom and at what time	Yes	REG	Transfer and sharing of personal data to third parties are recorded in the record of processing activities and in the logs of the respective applications.	Yes
Processor B.8.2.1	**Customer agreement**	The organization should 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	REG	Assistance to the controller defined in the DPA included in the General Terms and Conditions	Yes
Processor B.8.2.2	**Organization's purposes**	The organization should ensure that PII processed on behalf of a customer are only processed for the purposes expressed in the documented instructions of the customer	Yes	CON	Clauses ensuring that the data is only processed on behalf of the controller defined in the DPA included in the General Terms and Conditions	Yes
Processor B.8.2.3	**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	Yes	REG	Data for marketing purposes and handled according to the applicable laws and regualtions.	Yes
Processor B.8.2.4	**Infringing instruction**	The organization should inform the customer if, in its opinion, a processing instruction infringes applicable legislation and/or regulation	Yes	CON	Clauses ensuring that the processor will inform the controller of an instruction infringing the applicable legislation is inserted in the DPA included in the General Terms and Conditions	Yes
Processor B.8.2.5	**Customer obligations**	The organization should provide the customer with the appropriate information such that the customer can demonstrate compliance with their obligations	Yes	CON	Appropriate information is inserted in the DPA included in the General Terms and Conditions	Yes

ISO27701:19 Controls			Inclusion[1]		Justification	Implemented
Processor B.8.2.6	**Records related to processing of PII**	The organization should determine and securely maintain the necessary records in support of its obligations for the processing of PII	Yes	REG	Records of processing operations carried out on behalf of the controlelr are kept	Yes
Processor B.8.3.1	**Determining and fulfilling obligations to PII principals**	The organization should 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	REG	All processing operations carried out on behalf of the controller are documented.	Yes
Processor B.8.4.1	**Temporary files**	The organization should ensure that temporary files created as a result of the processing of PII are disposed of (e.g. erased or destroyed) following documented procedures within a specified, documented period	Yes	CON	Procedures implemented regarding the deletion of data and backup of data	Yes
Processor B.8.4.2	**Return, transfer or disposal of PII**	The organization should provide the ability to return, transfer and/or disposal of PII in a secure manner. It should also make its policy available to the customer	Yes	CON	Clauses inserted in the General Terms regulate the return of the data, including the format.	Yes
Processor B.8.4.3	**PII transmission controls**	The organization should 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	BP	efficy must transfer PII in a secure way, which is ensured through the implementation of technical solutions and role based access	Yes
Processor B.8.5.1	**Identify basis for PII transfer between jurisdictions**	The organization should identify and document the relevant basis for transfers of PII between jurisdictions	Yes	REG	Controller is informed of any transfer of data and suich transfer is documented in the list of sub-procesors	Yes

ISO27701:19 Controls			Inclusion[1]		Justification	Implemented
Processor B.8.5.2	**Countries and international organizations to which PII can be transferred**	The organization should specify and document the countries and international organizations to which PII can possibly be transferred	Yes	REG	Controller is informed of any transfer of data and suich transfer is documented in the list of sub-procesors	Yes
Processor B.8.5.3	**Records of PII disclosure to third parties**	The organization should record disclosures of PII to third parties, including what PII has been disclosed, to whom and at what time	Yes	REG	Controller is informed of any transfer of data and suich transfer is documented in the list of sub-procesors	Yes
Processor B.8.5.4	**Notification of PII Disclosure Requests**	The organization should notify the customer of any legally binding requests for disclosure of PII	Yes	REG	Clauses in the General Terms and Conditions provide that the customer shall be notifed in such cases	Yes
Processor B.8.5.5	**Legally Binding PII Disclosures**	The organization should 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	REG	No disclosure of personal data shall happen without the controller's instruction	Yes
Processor B.8.5.6	**Disclosure of subcontractors used to process PII**	The organization should disclose any use of subcontractors to process PII to the customer before use	Yes	REG	A list of subcontractors is inserted in the General Terms and Conditions	Yes
Processor B.8.5.7	**Engagement of a subcontractor to process PII**	The organization should only engage a subcontractor to process PII according to the customer contract	Yes	CON	Clauses in the DPA inserted in General Terms and Conditions provide the conditions under which a subcontractor can be engaged	Yes

ISO27701:19 Controls			Inclusion[1]		Justification	Implemented
Processor B.8.5.8	**Change of subcontractor to process PII**	The organization should, 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	CON	Clauses in the DPA inserted in General Terms and Conditions provide the conditions under which a subcontractor can be engaged	Yes