

ISO /IEC 27001

A.5 Organisatorische Maßnahmen / Organizational controls

Maßnahme	Anwendbar	Begründung	Umgesetzt
Control	Applicable	Justification	Implemented
ISO27-A.5.1 Informationssicherheitsrichtlinien / Policies for information security	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
ISO27-A.5.2 Informationssicherheits- und Datenschutzrollen und -verantwortlichkeiten / Information security roles and responsibilities	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
ISO27-A.5.3 Aufgabentrennung / Segregation of duties	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
ISO27-A.5.4 Verantwortlichkeiten der Leitung / Management responsibilities	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
ISO27-A.5.5 Kontakt mit Behörden / Contact with authorities	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
ISO27-A.5.6 Kontakt mit speziellen Interessensgruppen / Contact with special interest groups	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
ISO27-A.5.7 Informationen über Bedrohungen / Threat intelligence	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
ISO27-A.5.8 Informationssicherheit und Datenschutz im Projektmanagement / Information security in project management	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
ISO27-A.5.9 Inventarisierung von Informationen und anderen zugehörigen Werten / Inventory of information and other associated assets	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE

Maßnahme	Anwendbar	Begründung	Umgesetzt
Control	Applicable	Justification	Implemented
<p>ISO27-A.5.10</p> <p>Zulässiger Gebrauch von Informationen und anderen zugehörigen Werten / Acceptable use of information and other associated assets</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.5.11</p> <p>Rückgabe von Werten / Return of assets</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.5.12</p> <p>Klassifizierung von Information / Classification of information</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.5.13</p> <p>Kennzeichnung von Information / Labelling of information</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.5.14</p> <p>Informationsübertragung / Information transfer</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.5.15</p> <p>Zugangsteuerung / Access control</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.5.16</p> <p>Identitätsverwaltung / Identity management</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.5.17</p> <p>Authentifizierungsinformationen / Authentication information</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.5.18</p> <p>Zugriffsrechte / Access rights</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.5.19</p> <p>Informationssicherheits- und Datenschutzrichtlinie für Lieferantenbeziehungen / Information security in supplier relationships</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.5.20</p> <p>Behandlung von Sicherheit in Lieferantenvereinbarungen / Addressing information security within supplier agreements</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.5.21</p> <p>Lieferkette für Informations- und Kommunikationstechnologie / Managing information security in the ICT supply chain</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE

Maßnahme	Anwendbar	Begründung	Umgesetzt
Control	Applicable	Justification	Implemented
<p>ISO27-A.5.22</p> <p>Überwachung, Überprüfung und Änderungsmanagement von Lieferantenleistungen / Monitoring, review and change management of supplier services</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.5.23</p> <p>Informationssicherheit bei der Nutzung von Cloud-Diensten / Information security for use of cloud services</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.5.24</p> <p>Planung und Vorbereitung des Managements von Informationssicherheits- und Datenschutzvorfällen / Information security incident management planning and preparation</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.5.25</p> <p>Beurteilung von und Entscheidung über Informationssicherheits- und Datenschutzereignisse / Assessment and decision on information security events</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.5.26</p> <p>Reaktion auf Informationssicherheits- und Datenschutzvorfälle / Response to information security incidents</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.5.27</p> <p>Erkenntnisse aus Informationssicherheits- und Datenschutzvorfällen / Learning from information security incidents</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.5.28</p> <p>Sammeln von Beweismaterial / Collection of evidence</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.5.29</p> <p>Informationssicherheit und Datenschutz bei Störungen / Information security during disruption</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.5.30</p> <p>IT-Bereitschaft für die Betriebskontinuität / ICT readiness for business continuity</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.5.31</p> <p>Bestimmung der anwendbaren Gesetzgebung und der vertraglichen Anforderungen / Legal, statutory, regulatory and contractual requirements</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE

Maßnahme	Anwendbar	Begründung	Umgesetzt
Control	Applicable	Justification	Implemented
<p>ISO27-A.5.32</p> <p>Geistige Eigentumsrechte / Intellectual property rights</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.5.33</p> <p>Schutz von Aufzeichnungen / Protection of records</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.5.34</p> <p>Privatsphäre und Schutz von personenbezogener Information / Privacy and protection of PII</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.5.35</p> <p>Unabhängige Überprüfung der Informationssicherheit und des Datenschutzes / Independent review of information security</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.5.36</p> <p>Einhaltung von Sicherheits- und Datenschutzrichtlinien und -standards / Compliance with policies, rules and standards for information security</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.5.37</p> <p>Dokumentierte Bedienabläufe / Documented operating procedures</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE

A.6 Personenbezogene Maßnahmen / People controls

Maßnahme	Anwendbar	Begründung	Umgesetzt
Control	Applicable	Justification	Implemented
<p>ISO27-A.6.1</p> <p>Sicherheitsüberprüfung / Screening</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.6.2</p> <p>Beschäftigungs- und Vertragsbedingungen / Terms and conditions of employment</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.6.3</p> <p>Informationssicherheits- und Datenschutzbewusstsein, -ausbildung und -schulung / Information security awareness, education and training</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE

Maßnahme	Anwendbar	Begründung	Umgesetzt
Control	Applicable	Justification	Implemented
<p>ISO27-A.6.4</p> <p>Maßregelungsprozess / Disciplinary process</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.6.5</p> <p>Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung / Responsibilities after termination or change of employment</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.6.6</p> <p>Vertraulichkeits- oder Geheimhaltungsvereinbarungen / Confidentiality or non-disclosure agreements</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.6.7</p> <p>Telearbeit / Remote working</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.6.8</p> <p>Berichterstattung über Ereignisse im Bereich der Informationssicherheit und des Datenschutzes / Information security event reporting</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE

A.7 Physische Maßnahmen / Physical controls

Maßnahme	Anwendbar	Begründung	Umgesetzt
Control	Applicable	Justification	Implemented
<p>ISO27-A.7.1</p> <p>Physische Sicherheitsperimeter / Physical security perimeters</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.7.2</p> <p>Physische Zutrittssteuerung / Physical entry</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.7.3</p> <p>Sichern von Büros, Räumen und Einrichtungen / Securing offices, rooms and facilities</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.7.4</p> <p>Überwachung der physischen Sicherheit / Physical security monitoring</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE

Maßnahme	Anwendbar	Begründung	Umgesetzt
Control	Applicable	Justification	Implemented
<p>ISO27-A.7.5</p> <p>Schutz vor externen und umweltbedingten Bedrohungen / Protecting against physical and environmental threats</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.7.6</p> <p>Arbeiten in Sicherheitsbereichen / Working in secure areas</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.7.7</p> <p>Aufgeräumte Arbeitsumgebung und Bildschirmsperren / Clear desk and clear screen</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.7.8</p> <p>Platzierung und Schutz von Geräten und Betriebsmitteln / Equipment siting and protection</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.7.9</p> <p>Sicherheit von Geräten, Betriebsmitteln und Werten außerhalb der Räumlichkeiten / Security of assets off-premises</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.7.10</p> <p>Speichermedien / Storage media</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.7.11</p> <p>Versorgungseinrichtungen / Supporting utilities¹</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.7.12</p> <p>Sicherheit der Verkabelung / Cabling security</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.7.13</p> <p>Instandhalten von Geräten und Betriebsmitteln / Equipment maintenance</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.7.14</p> <p>Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln / Secure disposal or re-use of equipment</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE

A.8 Technologische Maßnahmen / Technological controls

Maßnahme	Anwendbar	Begründung	Umgesetzt
Control	Applicable	Justification	Implemented
<p>ISO27-A.8.1</p> <p>Benutzer-Endgeräte / User endpoint devices</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.8.2</p> <p>Verwaltung privilegierter Zugangsrechte / Privileged access rights</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.8.3</p> <p>Informationszugangsbeschränkung / Information access restriction</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.8.4</p> <p>Zugangsteuerung für Quellcode von Programmen / Access to source code</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.8.5</p> <p>Sichere Anmeldeverfahren / Secure authentication</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.8.6</p> <p>Kapazitätssteuerung / Capacity management</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.8.7</p> <p>Maßnahmen gegen Schadsoftware / Protection against malware</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.8.8</p> <p>Management von technischen Schwachstellen / Management of technical vulnerabilities</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.8.9</p> <p>Konfigurationsmanagement / Configuration management</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.8.10</p> <p>Löschung von Informationen / Information deletion</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.8.11</p> <p>Datenmaskierung / Data masking</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.8.12</p> <p>Verhinderung von Datenlecks / Data leakage prevention</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE

Maßnahme	Anwendbar	Begründung	Umgesetzt
Control	Applicable	Justification	Implemented
<p>ISO27-A.8.13</p> <p>Datensicherung / Information backup</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.8.14</p> <p>Verfügbarkeit von informationsverarbeitenden Einrichtungen / Redundancy of information processing facilities</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.8.15</p> <p>Ereignisprotokollierung / Logging</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.8.16</p> <p>Überwachung der Aktivitäten / Monitoring activities</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.8.17</p> <p>Uhrensynchronisation / Clock synchronization</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.8.18</p> <p>Gebrauch von Hilfsprogrammen mit privilegierten Rechten / Use of privileged utility programs</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.8.19</p> <p>Installation von Software auf Systemen im Betrieb / Installation of software on operational systems</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.8.20</p> <p>Sicherheit der Netzwerke / Networks security</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.8.21</p> <p>Sicherheit der Netzdienste / Security of network services</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.8.22</p> <p>Trennung von Netzwerken / Segregation of networks</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.8.23</p> <p>Internet-Filterung / Web filtering</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.8.24</p> <p>Gebrauch von Kryptographie / Use of cryptography</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE

Maßnahme	Anwendbar	Begründung	Umgesetzt
Control	Applicable	Justification	Implemented
<p>ISO27-A.8.25</p> <p>Sicherer Entwicklungslebenszyklus / Secure development life cycle</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.8.26</p> <p>Anforderungen an die Anwendungssicherheit / Application security requirements</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.8.27</p> <p>Sichere Systemarchitektur und technische Grundsätze / Secure system architecture and engineering principles</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.8.28</p> <p>Sichere Kodierung / Secure coding</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.8.29</p> <p>Sicherheitstests in Entwicklung und Abnahme / Security testing in development and acceptance</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.8.30</p> <p>Ausgliederte Entwicklung / Outsourced development</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.8.31</p> <p>Trennung von Entwicklungs-, Test- und Betriebsumgebungen / Separation of development, test and production environments</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.8.32</p> <p>Management von Änderungen / Change management</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.8.33</p> <p>Testdaten / Test information</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-A.8.34</p> <p>Schutz von Informationssystemen bei Prüfungen / Protection of information systems during audit testing</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE

ISO /IEC 27701

A.7 PIMS-spezifische Referenzmaßnahmenziele und -Maßnahmen (verantwortliche Stelle) / PIMS-specific reference measure objectives and controls (Controller)

Maßnahme	Anwendbar	Begründung	Umgesetzt
Control	Applicable	Justification	Implemented
A.7.2 Bedingungen für die Erhebung und Verarbeitung / Conditions for collection and processing			
<p>ISO27-27701-A.7.2.1</p> <p>Identifizieren und Dokumentieren des Zwecks / Identifying and documenting the purpose</p>	ja / yes	Gesetzliche Anforderung / Legal requirement	DONE
<p>ISO27-27701-A.7.2.2</p> <p>Identifizieren der rechtmäßigen Grundlage / Identifying the legal basis</p>	ja / yes	Gesetzliche Anforderung / Legal requirement	DONE
<p>ISO27-27701-A.7.2.3</p> <p>Bestimmen, wann und wie die Einwilligung einzuholen ist / Determine when and how to obtain consent</p>	ja / yes	Gesetzliche Anforderung / Legal requirement	DONE
<p>ISO27-27701-A.7.2.4</p> <p>Einholung und Aufzeichnung der Einwilligung / Obtaining and recording consent</p>	ja / yes	Gesetzliche Anforderung / Legal requirement	DONE
<p>ISO27-27701-A.7.2.5</p> <p>Datenschutz-Folgenabschätzung / Data protection impact assessment</p>	ja / yes	Gesetzliche Anforderung / Legal requirement	DONE
<p>ISO27-27701-A.7.2.6</p> <p>Verträge mit Auftragsverarbeitern / Contracts with processors</p>	ja / yes	Gesetzliche Anforderung / Legal requirement	DONE
<p>ISO27-27701-A.7.2.7</p> <p>Gemeinsame verantwortliche Stelle / Joint controllership</p>	ja / yes	Gesetzliche Anforderung / Legal requirement	DONE
<p>ISO27-27701-A.7.2.8</p> <p>Aufzeichnungen im Zusammenhang mit der Verarbeitung von personenbezogenen Daten / Records in connection with the processing of personal data</p>	ja / yes	Gesetzliche Anforderung / Legal requirement	DONE
A.7.3 Verpflichtungen gegenüber betroffenen Personen / Obligations towards data subjects			

Maßnahme	Anwendbar	Begründung	Umgesetzt
<p>ISO27-27701-A.7.3.1</p> <p>Bestimmung und Erfüllung von Verpflichtungen gegenüber betroffenen Personen / Determination and fulfillment of obligations towards data subjects</p>	ja / yes	Gesetzliche Anforderung / Legal requirement	DONE
<p>ISO27-27701-A.7.3.2</p> <p>Bestimmen von Informationen für betroffene Personen / Determining information for data subjects</p>	ja / yes	Gesetzliche Anforderung / Legal requirement	DONE
<p>ISO27-27701-A.7.3.3</p> <p>Bereitstellen von Informationen für betroffene Personen / Providing information for data subjects</p>	ja / yes	Gesetzliche Anforderung / Legal requirement	DONE
<p>ISO27-27701-A.7.3.4</p> <p>Bereitstellung eines Mechanismus zur Änderung oder zum Widerruf der Einwilligung / Provision of a mechanism for changing or withdrawing consent</p>	ja / yes	Gesetzliche Anforderung / Legal requirement	DONE
<p>ISO27-27701-A.7.3.5</p> <p>Bereitstellung eines Mechanismus zur Ablehnung der Verarbeitung personenbezogener Daten / Provision of a mechanism to object to the processing of personal data</p>	ja / yes	Gesetzliche Anforderung / Legal requirement	DONE
<p>ISO27-27701-A.7.3.6</p> <p>Zugriff, Korrektur und/oder Löschung / Access, correction and/or deletion</p>	ja / yes	Gesetzliche Anforderung / Legal requirement	DONE
<p>ISO27-27701-A.7.3.7</p> <p>Verpflichtungen von verantwortlichen Stellen, Dritte zu informieren / Obligations of processors to inform third parties</p>	ja / yes	Gesetzliche Anforderung / Legal requirement	DONE
<p>ISO27-27701-A.7.3.8</p> <p>Bereitstellung einer Kopie der verarbeiteten personenbezogenen Daten / Provision of a copy of the processed personal data</p>	ja / yes	Gesetzliche Anforderung / Legal requirement	DONE
<p>ISO27-27701-A.7.3.9</p> <p>Handhabung von Anfragen / Handling of requests</p>	ja / yes	Gesetzliche Anforderung / Legal requirement	DONE
<p>ISO27-27701-A.7.3.10</p> <p>Automatisierte Entscheidungsfindung / Automated decision-making process</p>	nein / no	Automatisierte Entscheidungsfindung wird nicht genutzt / Automated decision-making is not used	N/A
<p>A.7.4 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen / Data protection by design and by default</p>			

Maßnahme	Anwendbar	Begründung	Umgesetzt
<p>ISO27-27701-A.7.4.1</p> <p>Beschränkte Erhebung / Restricted collection</p>	ja / yes	Gesetzliche Anforderung / Legal requirement	DONE
<p>ISO27-27701-A.7.4.2</p> <p>Beschränkte Verarbeitung / Restricted processing</p>	ja / yes	Gesetzliche Anforderung / Legal requirement	DONE
<p>ISO27-27701-A.7.4.3</p> <p>Genauigkeit und Qualität / Accuracy and quality</p>	ja / yes	Gesetzliche Anforderung / Legal requirement	DONE
<p>ISO27-27701-A.7.4.4</p> <p>Ziele der Sparsamkeit personenbezogener Daten / Objectives of personal data minimization</p>	ja / yes	Gesetzliche Anforderung / Legal requirement	DONE
<p>ISO27-27701-A.7.4.5</p> <p>Entpersonalisierung personenbezogener Daten und Löschung am Ende der Verarbeitung / Depersonalization of personal data and deletion at the end of processing</p>	ja / yes	Gesetzliche Anforderung / Legal requirement	DONE
<p>ISO27-27701-A.7.4.6</p> <p>Temporäre Dateien / Temporary files</p>	ja / yes	Gesetzliche Anforderung / Legal requirement	DONE
<p>ISO27-27701-A.7.4.7</p> <p>Aufbewahrung / Storage</p>	ja / yes	Gesetzliche Anforderung / Legal requirement	DONE
<p>ISO27-27701-A.7.4.8</p> <p>Entsorgung / Disposal</p>	ja / yes	Gesetzliche Anforderung / Legal requirement	DONE
<p>ISO27-27701-A.7.4.9</p> <p>Maßnahmen zur Übertragung personenbezogener Daten / Measures for the transfer of personal data</p>	ja / yes	Gesetzliche Anforderung / Legal requirement	DONE
<p>A.7.5 Weitergabe, Übertragung und Offenlegung von personenbezogenen Daten / Forwarding, transfer and disclosure of personal data</p>			
<p>ISO27-27701-A.7.5.1</p> <p>Ermittlung der Grundlage für die Übertragung von personenbezogenen Daten zwischen Rechtssystemen / Determining the basis for the transfer of personal data between jurisdictions</p>	ja / yes	Gesetzliche Anforderung / Legal requirement	DONE

Maßnahme	Anwendbar	Begründung	Umgesetzt
<p>ISO27-27701-A.7.5.2</p> <p>Länder und internationale Organisationen, an die personenbezogene Daten übertragen werden können / Countries and international organizations to which personal data may be transferred</p>	ja / yes	Gesetzliche Anforderung / Legal requirement	DONE
<p>ISO27-27701-A.7.5.3</p> <p>Aufzeichnungen über die Übertragung von personenbezogenen Daten / Records of the transfer of personal data</p>	ja / yes	Gesetzliche Anforderung / Legal requirement	DONE
<p>ISO27-27701-A.7.5.4</p> <p>Aufzeichnungen der Offenlegung von personenbezogenen Daten für Dritte / Records of disclosure of personal data to third parties</p>	ja / yes	Gesetzliche Anforderung / Legal requirement	DONE

A.8 PIMS-spezifische Referenzmaßnahmenziele und -Maßnahmen (Auftragsverarbeiter) / PIMS-specific reference measure objectives and controls (Processor)

Maßnahme	Anwendbar	Begründung	Umgesetzt
Control	Applicable	Justification	Implemented
B.8.2 Bedingungen für die Erhebung und Verarbeitung / Conditions for collection and processing			
<p>ISO27-27701-B.8.2.1</p> <p>Kundenvereinbarung / Customer agreement</p>	ja / yes	Gesetzliche Anforderung / Legal requirement	DONE
<p>ISO27-27701-B.8.2.2</p> <p>Ziele der Organisation / Objectives of the organization</p>	ja / yes	Gesetzliche Anforderung / Legal requirement	DONE
<p>ISO27-27701-B.8.2.3</p> <p>Verwendung für Marketing und Werbung / Use for marketing and advertising</p>	ja / yes	Gesetzliche Anforderung / Legal requirement	DONE
<p>ISO27-27701-B.8.2.4</p> <p>Verstoßende Anweisung / Infringing instruction</p>	ja / yes	Gesetzliche Anforderung / Legal requirement	DONE
<p>ISO27-27701-B.8.2.5</p> <p>Kundenverpflichtungen / Customer obligations</p>	ja / yes	Gesetzliche Anforderung / Legal requirement	DONE

Maßnahme	Anwendbar	Begründung	Umgesetzt
<p>ISO27-27701-B.8.2.6</p> <p>Aufzeichnungen im Zusammenhang mit der Verarbeitung von personenbezogenen Daten / Records in connection with the processing of personal data</p>	ja / yes	Gesetzliche Anforderung / Legal requirement	DONE
B.8.3 Verpflichtungen gegenüber betroffenen Personen / Obligations towards data subjects			
<p>ISO27-27701-B.8.3.1</p> <p>Bestimmung und Erfüllung von Verpflichtungen gegenüber betroffenen Personen / Determination and fulfillment of obligations towards data subjects</p>	ja / yes	Gesetzliche Anforderung / Legal requirement	DONE
B.8.4 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen / Data protection by design and by default			
<p>ISO27-27701-B.8.4.1</p> <p>Temporäre Dateien / Temporary files</p>	ja / yes	Gesetzliche Anforderung / Legal requirement	DONE
<p>ISO27-27701-B.8.4.2</p> <p>Rückgabe, Übertragung oder Entsorgung von personenbezogenen Daten / Return, transfer or disposal of personal data</p>	ja / yes	Gesetzliche Anforderung / Legal requirement	DONE
<p>ISO27-27701-B.8.4.3</p> <p>Maßnahmen zur Übertragung personenbezogener Daten / Measures for the transfer of personal data</p>	ja / yes	Gesetzliche Anforderung / Legal requirement	DONE
B.8.5 Weitergabe, Übertragung und Offenlegung von personenbezogenen Daten / Forwarding, transfer and disclosure of personal data			
<p>ISO27-27701-B.8.5.1</p> <p>Grundlage für die Übertragung von personenbezogenen Daten zwischen Rechtssystemen / Basis for the transfer of personal data between jurisdictions</p>	ja / yes	Gesetzliche Anforderung / Legal requirement	DONE
<p>ISO27-27701-B.8.5.2</p> <p>Länder und internationale Organisationen, an die personenbezogene Daten übertragen werden können / Countries and international organizations to which personal data may be transferred</p>	ja / yes	Gesetzliche Anforderung / Legal requirement	DONE
<p>ISO27-27701-B.8.5.3</p> <p>Aufzeichnungen der Offenlegung von personenbezogenen Daten für Dritte / Records of disclosure of personal data to third parties</p>	ja / yes	Gesetzliche Anforderung / Legal requirement	DONE

Maßnahme	Anwendbar	Begründung	Umgesetzt
<p>ISO27-27701-B.8.5.4</p> <p>Benachrichtigung über Anträge auf Offenlegung von personenbezogenen Daten / Notification of requests for disclosure of personal data</p>	ja / yes	Gesetzliche Anforderung / Legal requirement	DONE
<p>ISO27-27701-B.8.5.5</p> <p>Rechtsverbindliche Offenlegung von personenbezogenen Daten / Legally binding disclosure of personal data</p>	ja / yes	Gesetzliche Anforderung / Legal requirement	DONE
<p>ISO27-27701-B.8.5.6</p> <p>Offenlegung von Unterauftragnehmern, die zur Verarbeitung von personenbezogenen Daten eingesetzt werden / Disclosure of subcontractors used for the processing of personal data</p>	ja / yes	Gesetzliche Anforderung / Legal requirement	DONE
<p>ISO27-27701-B.8.5.7</p> <p>Einschaltung eines Unterauftragnehmers mit der Verarbeitung von personenbezogenen Daten / Involvement of a subcontractor with the processing of personal data</p>	ja / yes	Gesetzliche Anforderung / Legal requirement	DONE
<p>ISO27-27701-B.8.5.8</p> <p>Wechsel des Unterauftragnehmers zur Verarbeitung von personenbezogenen Daten / Change of subcontractor for the processing of personal data</p>	ja / yes	Gesetzliche Anforderung / Legal requirement	DONE

Weitere Maßnahmen / Additional controls

Maßnahme	Anwendbar	Begründung	Umgesetzt
Control	Applicable	Justification	Implemented
<p>ISO27-OTHER-C.1</p> <p>Nutzung von Künstlicher Intelligenz / Use of artificial intelligence</p> <p>Die Organisation sollte eine themenspezifische Richtlinie für die Nutzung von KI-Systemen aufstellen. Der Ausschluss von hochkritischen KI-System sowie die Nutzung von Daten als Input und urheberrechtliche Aspekte sollten geregelt werden.</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE
<p>ISO27-OTHER-C.2</p> <p>Passwortmanager / Password manager</p> <p>Es sollten Regeln für die Nutzung von Passwortmanagern festgelegt und umgesetzt werden. Es sollte festgelegt werden, wann Passwortmanager einzusetzen sind und welche Anforderungen diese erfüllen müssen.</p>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	DONE