

## ISO /IEC 27001

### A.5 Organisatorische Maßnahmen / Organizational controls

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

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

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

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

## A.6 Personenbezogene Maßnahmen / People controls

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

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

## A.7 Physische Maßnahmen / Physical controls

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

Maßnahme	Anwendbar	Begründung	Umgesetzt
Control	Applicable	Justification	Implemented
<b>ISO27-A.7.5</b> Schutz vor externen und umweltbedingten Bedrohungen / Protecting against physical and environmental threats	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	<b>DONE</b>
<b>ISO27-A.7.6</b> Arbeiten in Sicherheitsbereichen / Working in secure areas	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	<b>DONE</b>
<b>ISO27-A.7.7</b> Aufgeräumte Arbeitsumgebung und Bildschirmsperren / Clear desk and clear screen	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	<b>DONE</b>
<b>ISO27-A.7.8</b> Platzierung und Schutz von Geräten und Betriebsmitteln / Equipment siting and protection	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	<b>DONE</b>
<b>ISO27-A.7.9</b> Sicherheit von Geräten, Betriebsmitteln und Werten außerhalb der Räumlichkeiten / Security of assets off-premises	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	<b>DONE</b>
<b>ISO27-A.7.10</b> Speichermedien / Storage media	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	<b>DONE</b>
<b>ISO27-A.7.11</b> Versorgungseinrichtungen / Supporting utilities <sup>1</sup>	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	<b>DONE</b>
<b>ISO27-A.7.12</b> Sicherheit der Verkabelung / Cabling security	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	<b>DONE</b>
<b>ISO27-A.7.13</b> Instandhalten von Geräten und Betriebsmitteln / Equipment maintenance	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	<b>DONE</b>
<b>ISO27-A.7.14</b> Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln / Secure disposal or re-use of equipment	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	<b>DONE</b>

## A.8 Technologische Maßnahmen / Technological controls

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

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



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

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

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

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

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

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

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

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>B.8.3 Verpflichtungen gegenüber betroffenen Personen / Obligations towards data subjects</b>			
<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>B.8.4 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen / Data protection by design and by default</b>			
<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>B.8.5 Weitergabe, Übertragung und Offenlegung von personenbezogenen Daten / Forwarding, transfer and disclosure of personal data</b>			
<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
<b>ISO27-27701-B.8.5.4</b> Benachrichtigung über Anträge auf Offenlegung von personenbezogenen Daten / Notification of requests for disclosure of personal data	ja / yes	Gesetzliche Anforderung / Legal requirement	<b>DONE</b>
<b>ISO27-27701-B.8.5.5</b> Rechtsverbindliche Offenlegung von personenbezogenen Daten / Legally binding disclosure of personal data	ja / yes	Gesetzliche Anforderung / Legal requirement	<b>DONE</b>
<b>ISO27-27701-B.8.5.6</b> Offenlegung von Unterauftragnehmern, die zur Verarbeitung von personenbezogenen Daten eingesetzt werden / Disclosure of subcontractors used for the processing of personal data	ja / yes	Gesetzliche Anforderung / Legal requirement	<b>DONE</b>
<b>ISO27-27701-B.8.5.7</b> Einschaltung eines Unterauftragnehmers mit der Verarbeitung von personenbezogenen Daten / Involvement of a subcontractor with the processing of personal data	ja / yes	Gesetzliche Anforderung / Legal requirement	<b>DONE</b>
<b>ISO27-27701-B.8.5.8</b> Wechsel des Unterauftragnehmers zur Verarbeitung von personenbezogenen Daten / Change of subcontractor for the processing of personal data	ja / yes	Gesetzliche Anforderung / Legal requirement	<b>DONE</b>

## Weitere Maßnahmen / Additional controls

Maßnahme	Anwendbar	Begründung	Umgesetzt
Control	Applicable	Justification	Implemented
<b>ISO27-OTHER-C.1</b> Nutzung von Künstlicher Intelligenz / Use of artificial intelligence 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.	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	<b>DONE</b>
<b>ISO27-OTHER-C.2</b> Passwortmanager / Password manager 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.	ja / yes	ISMS Risikoanalyse / ISMS Risk analysis	<b>DONE</b>