					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: PII24					Dokumenttitel: **Datenschutzrichtlinie für CCTV und physische Überwachung**							
Version: 1.0		Datum des Inkrafttretens: 01.01.2025			Dokumentenverantwortlicher:							
X	Richtlinie		Standard		Verfahren		Formular		Register		Sonstiges	

Änderungshistorie				
Änderungsnummer	**Änderungsdatum**	**Änderungen**	**Geprüft von**	**Prozessverantwortlicher**

Genehmigungen			
Name	**Position**	**Datum**	**Unterschrift**

Ausgerichtet an Standards und Vorschriften

Standard / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Dokumentierte und operative Kontrollen
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Überwachung und Korrekturmaßnahmen
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.9	Controller	Primary	Zweck, Rechtsgrundlage, Risikoauslöser und Aufzeichnungen
ISO/IEC 27701:2025	Annex A.1.2.7; Annex A.1.2.8	Controller	Supporting	Zuordnung von Auftragsverarbeiter und gemeinsam Verantwortlichem
ISO/IEC 27701:2025	Annex A.1.3.2; Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10	Controller	Supporting	Pflichten gegenüber betroffenen Personen und Anfragen
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5; Annex A.1.4.8; Annex A.1.4.9	Controller	Primary	Erhebung, Verarbeitung, Minimierung, Aufbewahrung und Entsorgung
ISO/IEC 27701:2025	Annex A.1.5.4; Annex A.1.5.5	Controller	Primary	Offenlegungsaufzeichnungen und Anfragen
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7	Processor	Supporting	Vereinbarungen, Weisungen, Unterstützung und Aufzeichnungen von Auftragsverarbeitern
ISO/IEC 27701:2025	Annex A.2.3.2; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Rechte von Auftragsverarbeitern und Unterstützung bei Offenlegungen
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Schutz von Aufzeichnungen und Protokollierung
GDPR	Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2)	Controller	Primary	Grundsätze und Rechenschaftspflicht
GDPR	Article 6	Controller	Primary	Rechtsgrundlage

GDPR	Article 12; Article 13; Article 14	Controller	Primary	Transparenz und Datenschutzhinweise
GDPR	Article 15; Article 16; Article 17; Article 18; Article 21	Controller	Supporting	Betroffenenanfragen
GDPR	Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39	Both	Supporting	Governance, Auftragsverarbeiter, Aufzeichnungen, Sicherheit, DPIA und Beratung
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Controller	Supporting	Zweck, Erhebung, Minimierung, Aufbewahrung und Offenlegung
ISO/IEC 29100:2020	Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12	Both	Supporting	Transparenz, Beteiligung, Rechenschaftspflicht, Sicherheit und Einhaltung
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2	Controller	Supporting	Datenschutzrisiko und DPIA-Auslöser
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10	Both	Supporting	Datenschutzkontrollen zum Schutz von PII
ISO/IEC 29151:2022	Clause 9.2.3; Clause 9.4.2; Clause 11.1.3	Both	Supporting	Zugriff und Kontrollen für physischen Zutritt
ISO/IEC 27002:2022	Controls 5.34; 7.2; 7.4; 8.2; 8.3; 8.15	Both	Supporting	PII, physische Überwachung, Zugriffsbeschränkung und Protokollierung

1. Geltungsbereich

1.1 Diese Richtlinie gilt für CCTV, Videoüberwachung, Besucherüberwachung, Protokolle der physischen Zutrittskontrolle, durch Sicherheitspersonal geführte Überwachungsaufzeichnungen, Systeme zur Überwachung von Betriebsstätten sowie damit verbundene physische Überwachungstätigkeiten, die PII erheben oder anderweitig verarbeiten.

1.2 Diese Richtlinie gilt für Organisationen, die als Verantwortliche für PII für ihre eigenen Betriebsstätten und physischen Überwachungstätigkeiten handeln.

1.3 Diese Richtlinie gilt außerdem für Unterstützungsleistungen als Auftragsverarbeiter oder Unterauftragsverarbeiter, wenn die Organisation Videoüberwachungsaufzeichnungen, Besucherdaten oder Protokolle der physischen Zutrittskontrolle im Auftrag eines Kunden betreibt, hostet, prüft, speichert, offenlegt, löscht oder anderweitig verarbeitet.

1.4 Diese Richtlinie umfasst die Festlegung des Überwachungszwecks, Genehmigung, Datenschutzhinweise und Hinweisschilder zur Überwachung, Zugriffsbeschränkungen, Offenlegung, Aufbewahrung, Löschung, Auslagerung, Vorfalleskalation, Weiterleitung von Betroffenenanfragen, Überprüfung und Management von Beweismitteln.

1.5 Diese Richtlinie enthält keine arbeitsrechtliche Beratung, keine rechtliche Kommentierung zu Betriebsräten, keine Verfahren für Strafverfolgungsbehörden und kein dediziertes CCTV-Register.

1.6 Überwachungsspezifische Nachweise werden in den kanonischen PIMS-Nachweisobjekten geführt, die in dieser Richtlinie benannt sind.

2. Zweck

2.1 Zweck dieser Richtlinie ist die Festlegung von Datenschutzkontrollen für CCTV und physische Überwachung, damit Überwachungstätigkeiten zweckgebunden, transparent, verhältnismäßig, zugriffskontrolliert, für definierte Zeiträume aufbewahrt, nur über genehmigte Kanäle offengelegt und durch auditierbare PIMS-Nachweise unterstützt werden.

2.2 Diese Richtlinie unterstützt den einheitlichen Umgang mit Videoüberwachungsaufzeichnungen, Besucheraufzeichnungen, Protokollen der physischen Zutrittskontrolle und zugehöriger Überwachungs-PII, ohne zusätzliche Register, Ausschüsse, Dashboards oder nicht kanonische Rollen zu schaffen.

3. Ziele

3.1 Die Ziele dieser Richtlinie sind:

3.1.1 Überwachungszwecke und Verarbeitungsumfang vor Beginn der Überwachung festzulegen;

3.1.2 CCTV, physische Zutrittskontrolle, Besucherüberwachung und physische Überwachungstätigkeiten in REG02 zu dokumentieren;

3.1.3 Überwachungstätigkeiten zu identifizieren, die eine Datenschutz-Risikobeurteilung oder ein DSFA-Screening in REG04 erfordern;

3.1.4 transparente Nachweise für Datenschutzhinweise und Hinweisschilder zur Überwachung in REG07 zu führen;

3.1.5 Zugriff, Einsichtnahme, Export, Offenlegung und Aufbewahrung von Überwachungs-PII zu beschränken;

3.1.6 Betroffenenanfragen über REG06 zu leiten;

3.1.7 ausgelagerte Überwachungsanbieter und Nachweise zur Datenweitergabe über REG08 zu verwalten;

3.1.8 vermutete Datenschutzvorfälle im Zusammenhang mit Überwachung über REG10 zu eskalieren;

3.1.9 Überprüfungen, Ausnahmen, Nichtkonformitäten, Korrekturmaßnahmen, Audit-Feststellungen und Verbesserungen in REG12 aufzuzeichnen.

4. Richtlinienaussagen

4.1 Überwachungsinventar, Zweck und Genehmigung

4.1.1 [Controller] The Process Owner / Business Owner MUSS jede CCTV-, Besucherüberwachungs-, physische Zutrittskontrollprotokoll- oder physische Überwachungstätigkeit in REG02 erfassen, bevor die Tätigkeit beginnt.

4.1.2 [Controller] The Privacy Lead / PIMS Manager MUSS den REG02-Eintrag für Zweck, Rechtsgrundlage, überwachten Standort, PII-Kategorien, Kategorien betroffener Personen, Aufbewahrung, Datenschutzhinweis, Zugriff und Offenlegungsfelder validieren, bevor eine neue oder wesentlich geänderte Überwachungstätigkeit aktiviert wird.

4.1.3 [Controller] The Process Owner / Business Owner MUSS genehmigte überwachte Zonen, ausgeschlossene Zonen und Erhebungsgrenzen in REG02 erfassen, bevor Kameras, Sensoren, Besucherprotokolle oder Protokollierung der Zutrittskontrolle aktiviert werden.

4.1.4 [Conditional] The Process Owner / Business Owner MUSS eine Datenschutzrisikoentscheidung in REG04 einholen, bevor Überwachung aktiviert wird, die systematische Überwachung, Audioaufzeichnung, biometrische Identifizierung, analysegestützte Erkennung, sensitive Standorte, schutzbedürftige Personen oder nicht offensichtliche Überwachung umfasst.

4.1.5 [Joint Controller] The Privacy Lead / PIMS Manager MUSS die Zuordnung der gemeinsamen Verantwortung für Überwachung in REG08 erfassen, bevor eine gemeinsame Überwachung mit einem Vermieter, Facility-Partner, Kunden oder einem anderen gemeinsam Verantwortlichen beginnt.

4.1.6 [Processor] The Privacy Lead / PIMS Manager MUSS Kundenweisungen zur Überwachung und zulässige Verarbeitungsgrenzen in REG08 erfassen, bevor Videoüberwachungsaufzeichnungen, Besucheraufzeichnungen oder Protokolle der physischen Zutrittskontrolle im Auftrag eines Kunden verarbeitet werden.

4.2 Datenschutzhinweis und Transparenz

4.2.1 [Controller] The Process Owner / Business Owner MUSS sicherstellen, dass Hinweisschilder zur Überwachung oder gleichwertige Nachweise für Just-in-time-Datenschutzhinweise in REG07 erfasst werden, bevor überwachte Bereiche für betroffene Personen geöffnet werden.

4.2.2 [Controller] The Privacy Lead / PIMS Manager MUSS jeden Überwachungs-Datenschutzhinweis in REG07 vor Veröffentlichung oder wesentlicher Änderung mit dem entsprechenden Verarbeitungszweck in REG02 verknüpfen.

4.2.3 [Processor] The Privacy Lead / PIMS Manager MUSS unterstützende Informationen zum Datenschutzhinweis für Überwachung in REG08 bereitstellen, wenn die Organisation Überwachungsdienste nach Kundenweisungen betreibt.

4.2.4 [Conditional] The Process Owner / Business Owner MUSS alternative Transparenzmaßnahmen in REG07 und REG04 erfassen, bevor nicht offensichtliche oder Notfallüberwachung aktiviert wird.

[... Abschnitte 4.3–8 sind in dieser Vorschau nicht enthalten. Erwerben Sie das vollständige Dokument, um auf den gesamten Inhalt zuzugreifen. ...]

9. Ausnahmen

9.1 [All] The Privacy Lead / PIMS Manager MUSS jede Ausnahme von dieser Richtlinie in REG12 erfassen, bevor die Ausnahme genutzt wird.

9.2 [Conditional] The Data Protection Officer / Privacy Advisor MUSS Datenschutzberatung in REG04 oder REG12 dokumentieren, bevor Ausnahmen genehmigt werden, die nicht offensichtliche Überwachung, Audioaufzeichnung, biometrische Identifizierung, analysegestützte Überwachung oder sensitive Überwachungsstandorte betreffen.

9.3 [All] Top Management MUSS Ausnahmen, die 90 Tage überschreiten, in REG12 genehmigen, bevor sie über den ursprünglichen Ausnahmezeitraum hinaus verlängert werden.

9.4 [All] The Privacy Lead / PIMS Manager MUSS offene Überwachungsausnahmen in REG12 mindestens monatlich bis zum Abschluss überprüfen.

10. Durchsetzung

10.1 [All] The Privacy Lead / PIMS Manager MUSS Versagen von Überwachungskontrollen innerhalb von fünf Geschäftstagen nach Bestätigung als Nichtkonformitäten in REG12 erfassen.

10.2 [Both] The Information Security Lead MUSS unbefugten Zugriff auf Überwachungssysteme innerhalb eines Geschäftstags nach Bestätigung aussetzen und die Maßnahme in REG10 oder REG12 erfassen.

10.3 [All] Top Management MUSS bei wiederholten oder wesentlichen Richtlinienverstößen die Verantwortlichkeit für Korrekturmaßnahmen innerhalb von 10 Geschäftstagen in REG12 zuweisen.

10.4 [Conditional] The Incident Response Coordinator MUSS bei vermuteter unbefugter Offenlegung, Verlust oder Kompromittierung von Überwachungs-PII den Workflow für PII-Vorfälle in REG10 einleiten.

11. Überprüfung und Pflege

11.1 [All] The Privacy Lead / PIMS Manager MUSS diese Richtlinie und die zugehörigen Überwachungsnachweise mindestens jährlich in REG12 überprüfen.

11.2 [Controller] The Process Owner / Business Owner MUSS jeden aktiven Überwachungszweck, Datenschutzhinweis, Standortumfang und Aufbewahrungseintrag mindestens jährlich in REG02 und REG07 erneut validieren.

11.3 [Both] The System Owner / Application Owner MUSS Zugriff, Protokollierung, Löschung und Exportkontrollen von Überwachungssystemen mindestens jährlich und nach wesentlichen Systemänderungen in REG12 erneut validieren.

11.4 [Conditional] The Vendor / Procurement Owner MUSS Nachweise zu ausgelagerten Überwachungsanbietern mindestens jährlich und vor Vertragsverlängerung in REG08 erneut validieren.

11.5 [All] The Privacy Lead / PIMS Manager MUSS zugehörige Nachweise in REG02, REG04, REG07, REG08, REG10 oder REG12 innerhalb von 30 Kalendertagen nach genehmigten Richtlinienänderungen aktualisieren.

12. Zugehörige Richtlinien

12.1 PII02 - Richtlinie zu Datenschutzrollen, Verantwortlichkeiten und Rechenschaftspflicht

12.2 PII03 - Richtlinie zum PII-Verarbeitungsinventar und zur Rechtsgrundlage

12.3 PII04 - Richtlinie zu Datenschutzhinweisen und Transparenz

12.4 PII06 - Richtlinie zum Management der Rechte betroffener Personen

12.5 PII07 - Richtlinie zur Datenschutz-Risikobeurteilung und DPIA

12.6 PII08 - Richtlinie zu Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

12.7 PII09 - Richtlinie zur Erhebung, Nutzung, Offenlegung und Weitergabe von PII

12.8 PII10 - Richtlinie zur Aufbewahrung, Löschung und Entsorgung von PII

12.9 PII12 - Richtlinie zum Datenschutzmanagement für Auftragsverarbeiter, Unterauftragsverarbeiter und Drittparteien

12.10 PII13 - Richtlinie zur internationalen Übermittlung personenbezogener Daten

12.11 PII14 - Richtlinie zu PII-Sicherheit und Zugriffskontrolle

12.12 PII15 - Richtlinie zum Management von PII-Vorfällen und PII-Verletzungen

12.13 PII17 - Richtlinie zum Management dokumentierter Information und Nachweise im PIMS

12.14 PII18 - Richtlinie zu PIMS-Überwachung, Audit und Verbesserung

12.15 PII19 - Datenschutzrichtlinie für Beschäftigte

12.16 PII21 - Datenschutzrichtlinie für KI und automatisierte Entscheidungsfindung

12.17 PII23 - Richtlinie für Cloud-PII-Auftragsverarbeiter

13. Referenzstandards und Rahmenwerke

13.1 Diese Richtlinie ist den folgenden Standards und Vorschriften zugeordnet. Die Zuordnung erläutert, wie die Richtlinie die genannten Anforderungen unterstützt, und identifiziert die internen Klauseln, die sie umsetzen oder unterstützen.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 7.5; Clause 8.1** - Zugeordnet zu dokumentierten Überwachungsnachweisen, operativer Planung, Aktivierungskontrollen, Zweckaufzeichnungen, Verknüpfung mit Datenschutzhinweisen, Zugriffskonfiguration, Aufbewahrungskonfiguration und Änderungssteuerung für CCTV und physische Überwachungstätigkeiten. Addressed by clauses [4.1.1; 4.1.2; 4.2.2; 4.3.1; 4.4.1; 6.2; 7.1; 11.5].

13.2.2 **Clause 9.1; Clause 10.2** - Zugeordnet zur Messung von Überwachungskontrollen, Anbieterüberprüfung, Berechtigungsüberprüfung, Audit-Feststellungen, Nichtkonformitäten, Korrekturmaßnahmen, Eskalation überfälliger Maßnahmen und Verbesserungsnachweisen. Addressed by clauses [4.6.4; 6.4; 6.5; 6.6; 8.1; 8.7; 10.1; 11.1].

13.2.3 **Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.9** - Zugeordnet zur Definition des Überwachungszwecks durch den Verantwortlichen, Dokumentation der Rechtsgrundlage, Entscheidungen zu Datenschutzrisikoauslösern und Aufzeichnungen zu Verarbeitungstätigkeiten der Überwachung in REG02 und REG04. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.4.1; 6.2; 7.1; 11.2].

13.2.4 **Annex A.1.2.7; Annex A.1.2.8** - Zugeordnet zur Zuordnung ausgelagerter Überwachungsanbieter, Zuordnung gemeinsamer Überwachungsverantwortung und Nachweisen zu Auftragsverarbeitern oder gemeinsam Verantwortlichen in REG08. Addressed by clauses [4.1.5; 4.6.1; 4.6.2; 5.7; 6.2; 7.6].

13.2.5 **Annex A.1.3.2; Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10** - Zugeordnet zu überwachungsbezogenen Pflichten gegenüber betroffenen Personen, Weiterleitung von Anfragen, erforderlicher Sicherung zur Bewertung von Anfragen und Governance-Nachweisen zur Unterstützung von Rechten. Addressed by clauses [4.5.1; 4.5.2; 5.2; 7.2; 11.5].

13.2.6 **Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5; Annex A.1.4.8; Annex A.1.4.9** - Zugeordnet zur Begrenzung der Überwachungserhebung, Verarbeitungsgrenzen, Minimierung, Aufbewahrungsfristen, Löschung, Überschreibung, Aufbewahrungssperren und Kontrolle extrahierter Kopien. Addressed by clauses [4.1.3; 4.3.1; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 7.3; 7.5; 8.4].

13.2.7 **Annex A.1.5.4; Annex A.1.5.5** - Zugeordnet zu Aufzeichnungen externer Offenlegungen, Bearbeitung von Offenlegungsersuchen, Minimierung vor Offenlegung und vorfallsbezogenen Offenlegungen mit Überwachungs-PII. Addressed by clauses [4.3.4; 4.5.4; 7.8; 10.4].

13.2.8 **Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7** - Zugeordnet zu Kundenweisungen für Auftragsverarbeiter, zulässigen Verarbeitungsgrenzen, Unterstützung für Datenschutzhinweise, Aufbewahrungs- und Löschweisungen, Unterstützung bei Rechten und Aufzeichnungen des Auftragsverarbeiters für ausgelagerte Überwachungsdienste. Addressed by clauses [4.1.6; 4.2.3; 4.4.5; 4.5.3; 4.6.3].

13.2.9 **Annex A.2.3.2; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6** - Zugeordnet zur Unterstützung des Auftragsverarbeiters für Kundenpflichten, Offenlegungsautorisierung, Offenlegungsaufzeichnungen, Benachrichtigung über Offenlegungsersuchen und Umgang mit rechtlich bindenden Offenlegungen für Überwachungs-PII. Addressed by clauses [4.3.5; 4.5.3; 4.6.2; 4.6.3].

13.2.10 **Annex A.3.14; Annex A.3.25** - Zugeordnet zum Schutz von Überwachungsaufzeichnungen, eingeschränktem Zugriff, Überprüfung privilegierter Zugriffe, Zugriffsprotokollierung, Eindämmung unbefugter Zugriffe und Protokollierungsnachweisen für Überwachungssysteme. Addressed by clauses [4.3.2; 4.3.3; 4.5.5; 5.4; 7.4; 10.2; 11.3].

13.3 GDPR

13.3.1 **Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2)** - Zugeordnet zu Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Speicherbegrenzung und Rechenschaftsnachweisen für Überwachungstätigkeiten. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.4.1; 4.4.2; 4.4.3; 6.1; 8.1; 11.2].

13.3.2 Article 6 - Zugeordnet zur Dokumentation der Rechtsgrundlage für CCTV, Besucherüberwachung, Protokolle der physischen Zutrittskontrolle und andere physische Überwachungstätigkeiten. Addressed by clauses [4.1.2; 4.1.4; 7.1].

13.3.3 **Article 12; Article 13; Article 14** - Zugeordnet zu transparenten Überwachungs-Datenschutzhinweisen, Nachweisen zu Hinweisschildern zur Überwachung, Verknüpfung von Datenschutzhinweisen mit Verarbeitungszwecken, unterstützenden Informationen zum Datenschutzhinweis durch Auftragsverarbeiter und alternativen Transparenzmaßnahmen. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 7.2; 8.2; 11.2].

13.3.4 **Article 15; Article 16; Article 17; Article 18; Article 21** - Zugeordnet zu Auskunft, Berichtigung, Löschung, Einschränkung, Widerspruch, Weiterleitung von Anfragen, erforderlicher Sicherung zur Bewertung von Anfragen und überwachungsbezogener Kundenunterstützung. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 7.8; 11.5].

13.3.5 **Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39** - Zugeordnet zu Governance des Verantwortlichen, Zuordnung gemeinsam Verantwortlicher, Governance von Auftragsverarbeitern, Verzeichnis von Verarbeitungstätigkeiten, Sicherheit von Überwachungssystemen, Datenschutz-Risikoprüfung, DPIA-Auslösern und Datenschutzberatung. Addressed by clauses [4.1.4; 4.1.5; 4.1.6; 4.3.2; 4.3.3; 4.5.4; 4.6.1; 4.6.2; 4.6.4; 5.1; 5.3; 6.3; 8.5; 10.4].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6** - Zugeordnet zu Zweckbestimmung, Begrenzung der Erhebung, Datenminimierung, Nutzungsbegrenzung, Aufbewahrungsbegrenzung und Offenlegungsbegrenzung für Überwachungs-PII. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.3.4; 4.4.1; 4.4.2; 4.4.4; 7.8].

13.4.2 **Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12** - Zugeordnet zu Transparenz, Beteiligung betroffener Personen, Rechenschaftspflicht, Informationssicherheit, Einhaltungsprüfung, Berechtigungsüberprüfung, Weiterleitung von Betroffenenanfragen,

Vorfalleskalation und Nachweisen zu Korrekturmaßnahmen. Addressed by clauses [4.2.1; 4.2.2; 4.3.2; 4.3.3; 4.5.1; 4.5.4; 6.1; 8.7; 10.1].

13.5 ISO/IEC 29134:2020

13.5.1 **Clause 5.1; Clause 6.2** - Zugeordnet zum Screening von Datenschutzrisiken und DPIA-Auslösern für systematische, nicht offensichtliche, audio-, biometrie- oder analysegestützte Überwachung, Überwachung sensibler Standorte, Überwachung schutzbedürftiger Personen oder andere physische Überwachung mit höherem Risiko. Addressed by clauses [4.1.4; 4.2.4; 5.3; 6.3; 7.5; 9.2].

13.6 ISO/IEC 29151:2022

13.6.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10** - Zugeordnet zu Datenschutzkontrollen zum Schutz von PII für Zweck, Erhebung, Minimierung, Aufbewahrung, Offenlegung und Beteiligung betroffener Personen in Überwachungskontexten. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.4.1; 4.4.3; 4.5.1; 7.2; 8.2].

13.6.2 **Clause 9.2.3; Clause 9.4.2; Clause 11.1.3** - Zugeordnet zur Zugriffsbereitstellung, Beschränkung des Informationszugriffs und Kontrollen des physischen Zutritts, die für den Zugriff auf Überwachungssysteme und Aufzeichnungen der physischen Zutrittskontrolle relevant sind. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.5.5; 5.4; 7.4; 10.2; 11.3].

13.7 ISO/IEC 27002:2022

13.7.1 Controls 5.34; 7.2; 7.4; 8.2; 8.3; 8.15 - Zugeordnet zum Datenschutz und Schutz von PII, physischem Zutritt, physischer Sicherheitsüberwachung, privilegiertem Zugriff, Beschränkung des Informationszugriffs und Protokollierungskontrollen für CCTV und physische Überwachungssysteme. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.5.5; 5.4; 7.3; 7.4; 8.3; 10.2; 11.3].