					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: PII24					Titolo del documento: **Politica privacy per videosorveglianza e monitoraggio fisico**							
Versione: 1.0		Data di entrata in vigore: 01.01.2025			Proprietario del documento:							
X	Politica		Standard		Procedura		Modulo		Registro		Altro	

Cronologia delle revisioni				
Numero di revisione	**Data di revisione**	**Modifiche**	**Riesaminato da**	**Proprietario del processo**

Approvazioni			
Nome	**Ruolo**	**Data**	**Firma**

Nota legale (diritti d'autore e limitazioni d'uso)

(C) 2025 Clarysec LLC. All rights reserved.

Il presente documento è proprietà intellettuale di Clarysec LLC. Nessuna parte del presente documento può essere copiata, riutilizzata, distribuita o modificata per finalità commerciali o di implementazione senza previa autorizzazione scritta espressa.

L'uso non autorizzato è severamente vietato e può comportare azioni legali.

Per richieste di licenza, contattare: info@clarysec.com

Allineamento a standard e normative applicabili

Standard / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Controlli documentati e operativi
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitoraggio e azione correttiva
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	Finalità, base giuridica, trigger di rischio e registrazioni
ISO/IEC 27701:2025	Annex A.1.2.7; Annex A.1.2.8	Controller	Supporting	Allocazione delle responsabilità del responsabile del trattamento e del contitolare del trattamento
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	Obblighi e richieste degli interessati
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	Raccolta, trattamento, minimizzazione, conservazione e smaltimento
ISO/IEC 27701:2025	Annex A.1.5.4; Annex A.1.5.5	Controller	Primary	Registrazioni e richieste relative alle comunicazioni
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	Accordi con responsabili del trattamento, istruzioni, supporto e registrazioni
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	Diritti del responsabile del trattamento e supporto alle comunicazioni
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Protezione delle registrazioni e logging
GDPR	Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2)	Controller	Primary	Principi e responsabilizzazione

GDPR	Article 6	Controller	Primary	Base giuridica
GDPR	Article 12; Article 13; Article 14	Controller	Primary	Trasparenza e informative
GDPR	Article 15; Article 16; Article 17; Article 18; Article 21	Controller	Supporting	Richieste di esercizio dei diritti
GDPR	Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39	Both	Supporting	Governance, responsabili del trattamento, registrazioni, sicurezza, DPIA e consulenza
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Controller	Supporting	Finalità, raccolta, minimizzazione, conservazione e comunicazione
ISO/IEC 29100:2020	Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12	Both	Supporting	Trasparenza, partecipazione, responsabilizzazione, sicurezza e conformità
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2	Controller	Supporting	Rischio privacy e trigger DPIA
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10	Both	Supporting	Controlli privacy per la protezione dei dati personali identificabili
ISO/IEC 29151:2022	Clause 9.2.3; Clause 9.4.2; Clause 11.1.3	Both	Supporting	Controlli di accesso e di ingresso fisico
ISO/IEC 27002:2022	Controls 5.34; 7.2; 7.4; 8.2; 8.3; 8.15	Both	Supporting	PII, monitoraggio fisico, restrizione degli accessi e logging

1. Ambito di applicazione

1.1 La presente politica si applica a videosorveglianza, monitoraggio video, monitoraggio dei visitatori, log di controllo degli accessi fisici, registrazioni di monitoraggio effettuato dal personale di vigilanza, sistemi di monitoraggio dei locali e attività correlate di monitoraggio fisico che raccolgono o altrimenti trattano PII.

1.2 La presente politica si applica alle organizzazioni che agiscono in qualità di titolari del trattamento per i PII dei propri locali e delle proprie attività di monitoraggio fisico.

1.3 Si applica inoltre alle attività di supporto svolte come responsabile del trattamento o sub-responsabile quando l'organizzazione gestisce, ospita, riesamina, archivia, comunica, cancella o altrimenti tratta registrazioni video di sorveglianza, dati dei visitatori o log degli accessi fisici per conto di un cliente.

1.4 La presente politica copre la definizione delle finalità del monitoraggio, l'approvazione, l'informativa e i cartelli informativi, le restrizioni di accesso, la comunicazione, la conservazione, la cancellazione, l'esternalizzazione, l'escalation degli incidenti, l'instradamento delle richieste di esercizio dei diritti, il riesame e la gestione delle evidenze.

1.5 La presente politica non fornisce consulenza in materia di diritto del lavoro, commenti giuridici relativi ai comitati aziendali, procedure per le forze dell'ordine o un registro dedicato alla videosorveglianza.

1.6 Le evidenze specifiche del monitoraggio sono mantenute negli elementi di evidenza canonici del PIMS identificati nella presente politica.

2. Finalità

2.1 La finalità della presente politica è stabilire controlli privacy per videosorveglianza e monitoraggio fisico affinché le attività di monitoraggio abbiano una finalità definita, siano trasparenti e proporzionate, siano soggette a controllo degli accessi, siano conservate per periodi definiti, siano comunicate solo tramite canali approvati e siano supportate da evidenze PIMS verificabili in sede di audit.

2.2 La presente politica supporta una gestione coerente delle registrazioni video di sorveglianza, delle registrazioni dei visitatori, dei log degli accessi fisici e dei relativi PII di monitoraggio senza creare ulteriori registri, comitati, dashboard o ruoli non canonici.

3. Obiettivi

3.1 Gli obiettivi della presente politica sono:

3.1.1 definire le finalità del monitoraggio e l'ambito del trattamento prima dell'avvio del monitoraggio;

3.1.2 documentare in REG02 le attività relative a videosorveglianza, accesso fisico, monitoraggio dei visitatori e monitoraggio fisico;

3.1.3 identificare in REG04 le attività di monitoraggio che richiedono un riesame del rischio privacy o uno screening DPIA;

3.1.4 mantenere in REG07 evidenze trasparenti relative all'informativa e ai cartelli informativi;

3.1.5 limitare l'accesso, la visualizzazione, l'esportazione, la comunicazione e la conservazione dei PII di monitoraggio;

3.1.6 instradare le richieste degli interessati tramite REG06;

3.1.7 gestire i fornitori di monitoraggio esternalizzati e le evidenze di condivisione dei dati tramite REG08;

3.1.8 segnalare tempestivamente tramite REG10 i sospetti incidenti relativi ai PII connessi al monitoraggio;

3.1.9 registrare in REG12 riesami, eccezioni, non conformità, azioni correttive, risultanze dell'audit e miglioramenti.

4. Dichiarazioni di politica

4.1 Inventario, finalità e approvazione del monitoraggio

4.1.1 [Controller] Il Process Owner / Business Owner deve registrare in REG02 ciascuna attività di videosorveglianza, monitoraggio dei visitatori, log di controllo degli accessi fisici o monitoraggio fisico prima dell'avvio dell'attività.

4.1.2 [Controller] Il Privacy Lead / PIMS Manager deve validare la voce REG02 relativa a finalità, base giuridica, luogo monitorato, categorie di PII, categorie di interessati, conservazione, informativa, accesso e campi di comunicazione prima dell'attivazione di una nuova attività di monitoraggio o di una sua modifica sostanziale.

4.1.3 [Controller] Il Process Owner / Business Owner deve registrare in REG02 le zone monitorate approvate, le zone escluse e i limiti di raccolta prima dell'abilitazione di telecamere, sensori, registri dei visitatori o registrazione del controllo degli accessi.

4.1.4 [Conditional] Il Process Owner / Business Owner deve ottenere una decisione sul rischio privacy in REG04 prima di attivare un monitoraggio che comporti monitoraggio sistematico, registrazione audio, identificazione biometrica, rilevamento abilitato da analytics, luoghi sensibili, persone vulnerabili o monitoraggio non evidente.

4.1.5 [Joint Controller] Il Privacy Lead / PIMS Manager deve registrare in REG08 l'allocazione delle responsabilità di monitoraggio congiunto prima dell'avvio del monitoraggio condiviso con un locatore, un partner per la gestione delle strutture, un cliente o altro contitolare del trattamento.

4.1.6 [Processor] Il Privacy Lead / PIMS Manager deve registrare in REG08 le istruzioni del cliente relative al monitoraggio e i limiti del trattamento consentito prima di trattare registrazioni video di sorveglianza, registrazioni dei visitatori o log degli accessi fisici per conto di un cliente.

4.2 Informativa e trasparenza

4.2.1 [Controller] Il Process Owner / Business Owner deve assicurare che l'evidenza dei cartelli informativi sul monitoraggio o di un'informativa just-in-time equivalente sia registrata in REG07 prima che le aree monitorate siano aperte agli interessati.

4.2.2 [Controller] Il Privacy Lead / PIMS Manager deve collegare ciascuna informativa sul monitoraggio in REG07 alla corrispondente finalità del trattamento in REG02 prima della pubblicazione o di una modifica sostanziale.

4.2.3 [Processor] Il Privacy Lead / PIMS Manager deve fornire in REG08 informazioni di supporto all'informativa sul monitoraggio quando l'organizzazione gestisce servizi di monitoraggio secondo le istruzioni del cliente.

4.2.4 [Conditional] Il Process Owner / Business Owner deve registrare misure alternative di trasparenza in REG07 e REG04 prima dell'attivazione di un monitoraggio non evidente o di emergenza.

[... Le sezioni 4.3–8 non sono incluse in questa anteprima. Acquistare il documento completo per accedere all'intero contenuto. ...]

9. Eccezioni

9.1 [All] Il Privacy Lead / PIMS Manager deve registrare ciascuna eccezione alla presente politica in REG12 prima che l'eccezione sia utilizzata.

9.2 [Conditional] Il Data Protection Officer / Privacy Advisor deve documentare la consulenza privacy in REG04 o REG12 prima dell'approvazione di eccezioni che riguardano monitoraggio non

evidente, registrazione audio, identificazione biometrica, monitoraggio abilitato da analytics o luoghi di monitoraggio sensibili.

9.3 [All] Top Management deve approvare in REG12 le eccezioni superiori a 90 giorni prima della proroga oltre il periodo iniziale di eccezione.

9.4 [All] Il Privacy Lead / PIMS Manager deve riesaminare in REG12 le eccezioni aperte relative al monitoraggio almeno mensilmente fino alla chiusura.

10. Applicazione della politica

10.1 [All] Il Privacy Lead / PIMS Manager deve registrare in REG12 i fallimenti dei controlli di monitoraggio come non conformità entro cinque giorni lavorativi dalla conferma.

10.2 [Both] L'Information Security Lead deve sospendere l'accesso non autorizzato al sistema di monitoraggio entro un giorno lavorativo dalla conferma e registrare l'azione in REG10 o REG12.

10.3 [All] Top Management deve assegnare in REG12 la titolarità delle azioni correttive entro 10 giorni lavorativi per violazioni ripetute o sostanziali della politica.

10.4 [Conditional] L'Incident Response Coordinator deve avviare il workflow degli incidenti PII in REG10 in caso di sospetta comunicazione non autorizzata, perdita o compromissione dei PII di monitoraggio.

11. Riesame e manutenzione

11.1 [All] Il Privacy Lead / PIMS Manager deve riesaminare la presente politica e le relative evidenze di monitoraggio in REG12 almeno annualmente.

11.2 [Controller] Il Process Owner / Business Owner deve riconvalidare in REG02 e REG07, almeno annualmente, ciascuna finalità di monitoraggio attiva, informativa, ambito geografico e voce di conservazione.

11.3 [Both] Il System Owner / Application Owner deve riconvalidare in REG12, almeno annualmente e dopo una modifica sostanziale del sistema, i controlli di accesso, logging, cancellazione ed esportazione del sistema di monitoraggio.

11.4 [Conditional] Il Vendor / Procurement Owner deve riconvalidare in REG08 le evidenze relative ai fornitori di monitoraggio esternalizzati almeno annualmente e prima del rinnovo contrattuale.

11.5 [All] Il Privacy Lead / PIMS Manager deve aggiornare le relative evidenze REG02, REG04, REG07, REG08, REG10 o REG12 entro 30 giorni di calendario dalle modifiche approvate della politica.

12. Politiche correlate

12.1 PII02 - Politica sui ruoli, sulle responsabilità e sulla responsabilizzazione privacy

12.2 PII03 - Politica sull'inventario dei trattamenti PII e sulla base giuridica

12.3 PII04 - Politica sulle informative privacy e sulla trasparenza

12.4 PII06 - Politica di gestione dei diritti degli interessati

12.5 PII07 - Politica di valutazione del rischio privacy e DPIA

12.6 PII08 - Politica di privacy by design e privacy by default

12.7 PII09 - Politica di raccolta, uso, comunicazione e condivisione dei PII

12.8 PII10 - Politica di conservazione, cancellazione e smaltimento dei PII

12.9 PII12 - Politica di gestione privacy di responsabili del trattamento, sub-responsabili e terze parti

12.10 PII13 - Politica sui trasferimenti internazionali di PII

12.11 PII14 - Politica di sicurezza e controllo degli accessi ai PII

12.12 PII15 - Politica di gestione degli incidenti e delle violazioni dei PII

12.13 PII17 - Politica sulle informazioni documentate e sulla gestione delle evidenze del PIMS

12.14 PII18 - Politica di monitoraggio, audit e miglioramento del PIMS

12.15 PII19 - Politica sulla privacy dei dipendenti

12.16 PII21 - Politica sulla privacy per IA e processi decisionali automatizzati

12.17 PII23 - Politica per responsabili del trattamento PII in cloud

13. Standard e quadri di riferimento

13.1 La presente politica è mappata ai seguenti standard e normative. La mappatura spiega in che modo la politica supporta i requisiti citati e identifica le clausole interne che li attuano o supportano.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 7.5; Clause 8.1** - Mappate alle evidenze documentate di monitoraggio, alla pianificazione operativa, ai controlli di attivazione, alle registrazioni delle finalità, al collegamento all'informativa, alla configurazione degli accessi, alla configurazione della conservazione e al controllo delle modifiche per le attività di videosorveglianza e monitoraggio fisico. 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** - Mappate alla misurazione dei controlli di monitoraggio, al riesame dei fornitori, al riesame degli accessi, alle risultanze dell'audit, alle non conformità, alle azioni correttive, all'escalation delle azioni scadute e alle evidenze di miglioramento. 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** - Mappate alla definizione delle finalità del monitoraggio da parte del titolare del trattamento, alla documentazione della base giuridica, alle decisioni sui trigger di rischio privacy e alle registrazioni delle attività di trattamento relative al monitoraggio in REG02 e 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** - Mappate all'allocazione dei fornitori di monitoraggio esternalizzati, all'allocazione delle responsabilità di monitoraggio congiunto e alle evidenze relative a responsabili del trattamento o contitolari del trattamento 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** - Mappate agli obblighi relativi agli interessati connessi al monitoraggio, all'instradamento delle richieste, alla conservazione necessaria per valutare le richieste e alle evidenze di governance a supporto dei diritti. 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** - Mappate alla limitazione della raccolta del monitoraggio, ai limiti del trattamento, alla minimizzazione, ai periodi di conservazione, alla cancellazione, alla sovrascrittura, ai blocchi della conservazione e al controllo delle copie estratte. 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** - Mappate alle registrazioni delle comunicazioni esterne, alla gestione delle richieste di comunicazione, alla minimizzazione prima della comunicazione e alle comunicazioni collegate a incidenti che coinvolgono PII di monitoraggio. 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** - Mappate alle istruzioni del cliente rivolte al responsabile del trattamento, ai limiti del trattamento consentito, al supporto all'informativa, alle istruzioni di conservazione e cancellazione, all'assistenza per i diritti e alle registrazioni del responsabile del trattamento per i servizi di monitoraggio esternalizzati. 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** - Mappate al supporto del responsabile del trattamento agli obblighi del cliente, all'autorizzazione alla comunicazione, alle registrazioni delle comunicazioni, alla notifica delle richieste di comunicazione e alla gestione delle comunicazioni giuridicamente vincolanti relative ai PII di monitoraggio. 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** - Mappate alla protezione delle registrazioni di monitoraggio, all'accesso limitato, al riesame degli accessi privilegiati, al logging degli accessi, al contenimento degli accessi non autorizzati e alle evidenze di logging per i sistemi di monitoraggio. 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)** - Mappate a liceità, correttezza, trasparenza, limitazione della finalità, minimizzazione dei dati, limitazione della conservazione ed evidenze di responsabilizzazione per le attività di monitoraggio. 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 - Mappato alla documentazione della base giuridica per videosorveglianza, monitoraggio dei visitatori, log degli accessi fisici e altre attività di monitoraggio fisico. Addressed by clauses [4.1.2; 4.1.4; 7.1].

13.3.3 **Article 12; Article 13; Article 14** - Mappati a informative di monitoraggio trasparenti, evidenze dei cartelli informativi, collegamento dell'informativa alle finalità del trattamento, informazioni di supporto all'informativa fornite dal responsabile del trattamento e misure alternative di trasparenza. 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** - Mappati ad accesso, rettifica, cancellazione, limitazione, opposizione, instradamento delle richieste, conservazione necessaria per valutare le richieste e assistenza al cliente relativa al monitoraggio. 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** - Mappati a governance del titolare del trattamento, allocazione del contitolare del trattamento, governance del responsabile del trattamento, registrazioni dei trattamenti, sicurezza dei sistemi di monitoraggio, riesame del rischio privacy, trigger DPIA e consulenza privacy. 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** - Mappate alla specificazione della finalità, alla limitazione della raccolta, alla minimizzazione dei dati, alla limitazione dell'uso, alla limitazione della conservazione e alla limitazione della comunicazione per i PII di monitoraggio. 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** - Mappate a trasparenza, partecipazione individuale, responsabilizzazione, sicurezza delle informazioni, riesame della conformità, riesame degli accessi, instradamento dei diritti, escalation degli incidenti ed evidenze di azioni correttive. 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** - Mappate allo screening dei trigger di rischio privacy e DPIA per monitoraggio sistematico, non evidente, audio, biometrico, abilitato da analytics, in luoghi sensibili, relativo a persone vulnerabili o altro monitoraggio fisico a rischio più elevato. 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** - Mappate ai controlli di protezione dei PII per finalità, raccolta, minimizzazione, conservazione, comunicazione e partecipazione degli interessati nei contesti di monitoraggio. 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** - Mappate al provisioning degli accessi, alla restrizione dell'accesso alle informazioni e ai controlli di ingresso fisico pertinenti per l'accesso ai sistemi di monitoraggio e per le registrazioni del controllo degli accessi fisici. 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 - Mappati alla privacy e alla protezione dei PII, all'ingresso fisico, al monitoraggio della sicurezza fisica, agli accessi privilegiati, alla restrizione dell'accesso alle informazioni e ai controlli di logging per i sistemi di videosorveglianza e monitoraggio fisico. 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].