

				Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: PII21				Titolo del documento: Politica privacy per l'IA e il processo decisionale automatizzato							
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

<p>Nota legale (diritti d'autore e limitazioni d'uso) (C) 2025 Clarysec LLC. All rights reserved.</p> <p>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.</p> <p>L'uso non autorizzato è severamente vietato e può comportare azioni legali.</p> <p>Per richieste di licenza, contattare: info@clarysec.com</p>
--

Allineamento a standard e normative applicabili

Standard / normativa	Clausola / controllo / articolo	Applicabilità	Tipo di copertura	Commento
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Informazioni documentate e controllo operativo per le evidenze relative al trattamento con IA, profilazione e processo decisionale automatizzato
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitoraggio, non conformità e azione correttiva per i controlli privacy relativi all'IA
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, valutazione d'impatto sulla privacy e registrazioni del titolare del trattamento
ISO/IEC 27701:2025	Annex A.1.2.7; Annex A.1.2.8	Controller	Supporting	Contratti con i responsabili del trattamento e responsabilità dei contitolari del trattamento per il trattamento di PII relativo all'IA
ISO/IEC 27701:2025	Annex A.1.3.2; Annex A.1.3.3; Annex A.1.3.4	Controller	Primary	Obblighi verso gli interessati e trasparenza per il trattamento relativo all'IA
ISO/IEC 27701:2025	Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10; Annex A.1.3.11	Controller	Primary	Obblighi relativi a opposizione, accesso, rettifica, cancellazione, gestione delle richieste e processo decisionale automatizzato
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5	Controller	Primary	Limiti di raccolta, trattamento e minimizzazione per

				input, output e dati derivati dell'IA
ISO/IEC 27701:2025	Annex A.1.5.2; Annex A.1.5.3; Annex A.1.5.4; Annex A.1.5.5	Conditional	Supporting	Instradamento dei trasferimenti internazionali, delle comunicazioni e delle richieste di comunicazione di PII relativi all'IA
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	Primary	Accordo con il responsabile del trattamento, istruzioni documentate, supporto agli obblighi del cliente e registrazioni
ISO/IEC 27701:2025	Annex A.2.3.2; Annex A.2.5.2; Annex A.2.5.3; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Supporto del responsabile del trattamento per gli obblighi verso gli interessati, l'instradamento dei trasferimenti e la gestione delle comunicazioni
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Protezione delle registrazioni e logging relativi al trattamento di PII connesso all'IA
GDPR	Article 4(4); Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(d); Article 5(2)	Controller	Primary	Profilazione, correttezza, trasparenza, limitazione della finalità, minimizzazione, esattezza e responsabilizzazione
GDPR	Article 6; Article 9; Article 10	Controller	Primary	Liceità, dati appartenenti a categorie particolari e misure di protezione per dati relativi a condanne penali o reati
GDPR	Article 12; Article 13; Article 14; Article 15	Controller	Primary	Informazioni trasparenti, accesso e informazioni significative sul

				processo decisionale automatizzato
GDPR	Article 16; Article 17; Article 18; Article 21; Article 22	Controller	Primary	Diritti di rettifica, cancellazione, limitazione, opposizione e relativi al processo decisionale automatizzato
GDPR	Article 24; Article 25; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39	Both	Supporting	Responsabilità del titolare del trattamento, protezione dei dati fin dalla progettazione e per impostazione predefinita, contitolari, responsabili del trattamento, registrazioni, sicurezza, DPIA e compiti del DPO
GDPR	Article 44	Conditional	Referenced	Instradamento dei trasferimenti internazionali per il trattamento di PII relativo all'IA
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.7	Both	Primary	Principi di finalità, raccolta, minimizzazione, uso, conservazione, comunicazione, esattezza e qualità
ISO/IEC 29100:2020	Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12	Both	Supporting	Trasparenza, partecipazione individuale, responsabilizzazione, sicurezza delle informazioni e conformità privacy
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2; Clause 6.3	Both	Supporting	Benefici della PIA, determinazione della soglia e preparazione alla valutazione del rischio privacy relativo all'IA
ISO/IEC 29151:2022	Annex A.4; Annex A.5; Annex A.7;	Both	Supporting	Controlli relativi a finalità, raccolta,

	Annex A.8; Annex A.10			minimizzazione, uso, conservazione, comunicazione, esattezza e partecipazione dell'interessato
--	-----------------------	--	--	--

1. Ambito di applicazione

1.1 La presente politica definisce i requisiti privacy obbligatori per le attività di trattamento basate su intelligenza artificiale, profilazione, attribuzione di punteggi, raccomandazione, supporto decisionale e processo decisionale automatizzato che utilizzano, inferiscono, generano, comunicano o trattano in altro modo PII nell'ambito di applicazione del PIMS.

1.2 La presente politica si applica a:

1.2.1 sistemi, applicazioni, modelli, servizi, workflow, motori decisionali, strumenti di attribuzione di punteggi, sistemi di raccomandazione, modelli di analisi e processi decisionali automatizzati abilitati dall'IA che trattano PII;

1.2.2 profilazione, segmentazione, classificazione, previsione, inferenza, personalizzazione, classificazione in graduatoria, idoneità, rilevazione delle frodi, attribuzione di punteggi di rischio, decisioni di accesso, valutazione relativa al rapporto di lavoro, profilazione relativa a minori, personalizzazione del marketing e trattamenti analoghi nei quali sono coinvolte PII;

1.2.3 PII relative all'IA utilizzate per addestramento, test, validazione, tuning, monitoraggio, inferenza in produzione, riesame degli output, misurazione delle prestazioni, indagine sugli incidenti o ritiro del modello;

1.2.4 contesti di titolare del trattamento, contitolare del trattamento, responsabile del trattamento e sub-responsabile;

1.2.5 fornitori, responsabili del trattamento, sub-responsabili, destinatari di condivisione dei dati e rotte di trasferimento internazionale relativi all'IA che trattano PII.

1.3 La presente politica non istituisce un quadro completo di governance dell'IA, un sistema di gestione dell'IA, un inventario dell'IA, un inventario dei modelli, un registro dei rischi dei modelli, un registro di fairness, un registro degli algoritmi, un registro degli incidenti IA, un comitato IA, un ruolo di proprietario del modello, un ruolo di proprietario del sistema IA, un workflow di consulenza legale o un modulo separato di approvazione dell'IA.

1.4 La presente politica non sostituisce:

1.4.1 PII03 per inventario dei trattamenti, base giuridica e titolarità del ROPA;

1.4.2 PII04 per la governance dell'informativa privacy;

1.4.3 PII05 per la gestione del consenso e delle preferenze;

1.4.4 PII06 per il workflow relativo ai diritti degli interessati;

1.4.5 PII07 per la valutazione del rischio privacy e la metodologia DPIA;

1.4.6 PII08 per i gate di privacy by design e privacy by default;

1.4.7 PII09 per i controlli su raccolta, uso, comunicazione e condivisione;

1.4.8 PII10 per l'esecuzione di conservazione, cancellazione e smaltimento;

1.4.9 PII11 per i controlli di esattezza e qualità;

1.4.10 PII12 per la governance del ciclo di vita di responsabili del trattamento, sub-responsabili e terze parti;

1.4.11 PII13 per i controlli sui trasferimenti internazionali;

1.4.12 PII14 per la sicurezza e il controllo degli accessi;

1.4.13 PII15 per la gestione degli incidenti e delle violazioni;

1.4.14 PII18 per monitoraggio, audit e miglioramento;

1.4.15 PII19 per la privacy dei dipendenti;

1.4.16 PII20 per la privacy dei minori;

1.4.17 PII22 per la privacy nel marketing e i cookie.

2. Finalità

- 2.1 La finalità della presente politica è garantire che le attività di IA, profilazione e processo decisionale automatizzato che coinvolgono PII siano identificate, documentate, sottoposte a valutazione del rischio, trasparenti, contestabili, monitorate e controllate tramite il PIMS, senza creare artifact di governance duplicati specifici per l'IA.
- 2.2 La presente politica garantisce che gli obblighi privacy relativi al trattamento di PII connesso all'IA siano dimostrati tramite REG02, REG04, REG06, REG07, REG08, REG09, REG10 e REG12.

3. Obiettivi

3.1 Gli obiettivi della presente politica sono:

- 3.1.1 identificare in REG02 i trattamenti di IA, profilazione e processo decisionale automatizzato che coinvolgono PII;
- 3.1.2 documentare in REG02 finalità relative all'IA, base giuridica, categorie di PII, fonti dei dati, dati inferiti, output, destinatari ed effetti decisionali;
- 3.1.3 attivare lo screening del rischio privacy e l'instradamento della DPIA tramite REG04;
- 3.1.4 assicurare che le informative privacy relative all'IA e le informazioni significative siano registrate in REG07;
- 3.1.5 instradare le richieste relative a diritti, opposizione, riesame umano e contestabilità tramite REG06;
- 3.1.6 controllare responsabili del trattamento, sub-responsabili, fornitori e accordi di condivisione dei dati relativi all'IA tramite REG08;
- 3.1.7 instradare i trasferimenti internazionali relativi all'IA tramite REG09;
- 3.1.8 segnalare tempestivamente sospetti incidenti relativi a PII connessi all'IA, uso improprio, comunicazione non autorizzata ed esiti privacy avversi tramite REG10 e REG12;
- 3.1.9 registrare monitoraggio, eccezioni, non conformità, azioni correttive e miglioramenti in REG12.

4. Dichiarazioni della politica

4.1 Identificazione di IA, profilazione e processo decisionale automatizzato

- 4.1.1 [Controller] Quando viene proposto un sistema, un'applicazione, un modello, un workflow, un servizio o un processo aziendale nuovo o modificato in modo sostanziale, il Process Owner / Business Owner deve determinare se utilizza IA, profilazione, attribuzione di punteggi, raccomandazione, supporto decisionale o processo decisionale automatizzato che coinvolge PII e registrare la determinazione in REG02.
- 4.1.2 [Controller] Prima dell'avvio del trattamento di PII relativo all'IA, il Process Owner / Business Owner deve documentare in REG02 la finalità del trattamento, le categorie di PII, le categorie di interessati, le fonti dei dati, le categorie di dati inferiti o derivati, le categorie di output, le categorie di destinatari, la base giuridica e il collegamento con la conservazione.
- 4.1.3 [Controller] Prima che profilazione, attribuzione di punteggi, raccomandazione, supporto decisionale o processo decisionale automatizzato siano utilizzati in produzione, il Process Owner / Business Owner deve documentare in REG02 e REG04 il contesto decisionale, l'effetto atteso sugli interessati, il coinvolgimento umano e il percorso per l'esercizio dei diritti.
- 4.1.4 [Joint Controller] Prima che il trattamento di PII relativo all'IA sia svolto con un contitolare del trattamento, il Privacy Lead / PIMS Manager deve documentare in REG08 la responsabilità per la definizione della finalità, l'informativa, la gestione dei diritti, il supporto alla DPIA, la governance dei responsabili del trattamento e l'escalation degli incidenti.
- 4.1.5 [Processor] Prima di trattare PII tramite un servizio relativo all'IA per un cliente, il Process Owner / Business Owner deve confermare che le istruzioni del cliente, le finalità consentite, gli usi vietati, la gestione degli output e gli obblighi di assistenza siano documentati in REG08.

4.1.6 [Both] Prima dell'attivazione del trattamento di PII relativo all'IA, il Privacy Lead / PIMS Manager deve confermare che il trattamento sia collegato agli elementi di evidenza canonici applicabili e che non sia creato alcun registro separato specifico per l'IA al di fuori di REG02, REG04, REG06, REG07, REG08, REG09, REG10 o REG12.

4.2 Valutazione del rischio privacy e instradamento della DPIA

4.2.1 [Controller] Prima di avviare o modificare in modo sostanziale un trattamento di PII relativo all'IA, il Privacy Lead / PIMS Manager deve completare lo screening del rischio privacy e registrare la decisione sulla DPIA in REG04.

4.2.2 [Conditional] Quando il trattamento relativo all'IA comporta profilazione, decisioni automatizzate, valutazione su larga scala, dati appartenenti a categorie particolari, dati relativi a reati, interessati vulnerabili, valutazione dei dipendenti, minori, monitoraggio comportamentale, dati di localizzazione, dati biometrici, attribuzione di punteggi ad alto impatto o effetti significativi, il Data Protection Officer / Privacy Advisor deve riesaminare il rischio privacy e registrare il parere in REG04.

4.2.3 [Controller] Prima della messa in esercizio in produzione di un trattamento di PII relativo all'IA, il Process Owner / Business Owner deve documentare in REG04 o REG12 le azioni di trattamento del rischio, lo stato del rischio residuo e le evidenze di prontezza alla messa in esercizio.

4.2.4 [Controller] Prima che le PII siano riutilizzate per addestramento, test, validazione, tuning, monitoraggio o miglioramento del modello IA per una finalità nuova o modificata in modo sostanziale, il Process Owner / Business Owner deve completare il riesame privacy e registrare la decisione in REG02 e REG04.

4.2.5 [Conditional] Quando il rischio privacy residuo resta elevato dopo il trattamento pianificato, Top Management deve approvare, respingere o richiedere un ulteriore trattamento prima dell'uso in produzione e registrare la decisione in REG04 e REG12.

[... 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] Prima di discostarsi da un requisito privacy relativo all'IA contenuto nella presente politica, il Process Owner / Business Owner richiedente deve presentare in REG12 la motivazione dell'eccezione e le evidenze dei controlli compensativi.

9.2 [Conditional] Quando un'eccezione incide su profilazione, processo decisionale automatizzato, riesame umano, contestabilità, trasparenza, esito della DPIA, attribuzione di punteggi ad alto impatto, trattamento relativo a minori, trattamento relativo a dipendenti, restrizioni dei responsabili del trattamento o trasferimenti internazionali, il Data Protection Officer / Privacy Advisor deve riesaminare l'eccezione e registrare il parere in REG04 o REG12.

9.3 [Conditional] Quando un'eccezione crea o mantiene un rischio privacy residuo elevato, Top Management deve approvare o respingere l'eccezione e registrare la decisione in REG04 e REG12.

9.4 [All] Prima della scadenza di un'eccezione privacy relativa all'IA approvata, il Privacy Lead / PIMS Manager deve riesaminare lo stato di chiusura, rinnovo o azione correttiva e registrare l'esito in REG12.

10. Applicazione della politica

10.1 [All] Quando viene identificata una non conformità alla presente politica, il Privacy Lead / PIMS Manager deve registrare la non conformità e l'azione correttiva in REG12.

- 10.2 [Both] Quando si sospetta trattamento, comunicazione o accesso non autorizzato a PII relativi all'IA, uso improprio del modello, mancata gestione dei diritti o esito privacy avverso, l'Incident Response Coordinator deve avviare l'escalation dell'incidente e registrare le evidenze in REG10 e REG12.
- 10.3 [Both] Quando un responsabile del trattamento, sub-responsabile, fornitore o destinatario di condivisione dei dati non soddisfa gli obblighi privacy relativi all'IA, il Vendor / Procurement Owner deve registrare in REG08 e REG12 l'azione di rimedio, escalation o risoluzione.
- 10.4 [All] Quando si verificano non conformità privacy relative all'IA ripetute o sistemiche, Top Management deve riesaminare la questione e registrare l'azione della direzione in REG12.

11. Riesame e manutenzione

- 11.1 [All] Almeno annualmente, il Privacy Lead / PIMS Manager deve riesaminare la presente politica per verificarne la continua idoneità e registrare l'esito del riesame in REG12.
- 11.2 [Conditional] Quando leggi, servizi, modelli, fonti di dati, pratiche di profilazione, logica del processo decisionale automatizzato, accordi con i fornitori, rotte di trasferimento o rischi privacy cambiano in modo sostanziale, il Privacy Lead / PIMS Manager deve riesaminare i controlli privacy relativi all'IA interessati e registrare l'esito in REG02, REG04 o REG12.
- 11.3 [Controller] Almeno annualmente e dopo modifiche sostanziali del percorso utente relativo all'IA, il Process Owner / Business Owner deve riesaminare le evidenze relative a trasparenza, informazioni significative, riesame umano e percorso per l'esercizio dei diritti e registrare il riesame in REG06 e REG07.
- 11.4 [All] Dopo la chiusura delle azioni correttive privacy relative all'IA, l'Internal Audit / Compliance Reviewer deve verificarne l'efficacia e registrare le evidenze di verifica in REG12.

12. Politiche correlate

- 12.1 PII01 - Politica del Sistema di gestione delle informazioni sulla privacy
- 12.2 PII02 - Politica sui ruoli, le responsabilità e la responsabilizzazione in materia di privacy
- 12.3 PII03 - Politica sull'inventario dei trattamenti di PII e sulla base giuridica
- 12.4 PII04 - Politica sull'informativa privacy e sulla trasparenza
- 12.5 PII05 - Politica di gestione del consenso e delle preferenze
- 12.6 PII06 - Politica di gestione dei diritti degli interessati
- 12.7 PII07 - Politica di valutazione del rischio privacy e DPIA
- 12.8 PII08 - Politica di privacy by design e privacy by default
- 12.9 PII09 - Politica sulla raccolta, l'uso, la comunicazione e la condivisione di PII
- 12.10 PII10 - Politica di conservazione, cancellazione e smaltimento delle PII
- 12.11 PII11 - Politica sull'esattezza e sulla qualità delle PII
- 12.12 PII12 - Politica di gestione privacy di responsabili del trattamento, sub-responsabili e terze parti
- 12.13 PII13 - Politica sui trasferimenti internazionali di PII
- 12.14 PII14 - Politica sulla sicurezza e sul controllo degli accessi alle PII
- 12.15 PII15 - Politica di gestione degli incidenti e delle violazioni delle PII
- 12.16 PII17 - Politica sulle informazioni documentate e sulla gestione delle evidenze del PIMS
- 12.17 PII18 - Politica di monitoraggio, audit e miglioramento del PIMS
- 12.18 PII19 - Politica sulla privacy dei dipendenti
- 12.19 PII20 - Politica sulla privacy dei minori
- 12.20 PII22 - Politica sulla privacy nel marketing e sui cookie

13. Standard e quadri di riferimento

- 13.1 ISO/IEC 27701:2025 - Clause 7.5; Clause 8.1. Addressed by clauses [4.1.6; 4.8.1; 6.1; 7.1; 7.5; 11.1].
- 13.2 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.6.2; 4.6.5; 4.8.2; 6.5; 8.1; 8.2; 8.3; 8.4; 8.5; 10.1; 11.4].
- 13.3 ISO/IEC 27701:2025 - Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.9. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.2.3; 4.2.4; 4.8.1; 7.1; 7.2].
- 13.4 ISO/IEC 27701:2025 - Annex A.1.2.7; Annex A.1.2.8. Addressed by clauses [4.1.4; 4.7.1; 4.7.2; 4.7.3; 5.7; 6.3; 7.6].
- 13.5 ISO/IEC 27701:2025 - Annex A.1.3.2; Annex A.1.3.3; Annex A.1.3.4. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 7.3; 11.3].
- 13.6 ISO/IEC 27701:2025 - Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10; Annex A.1.3.11. Addressed by clauses [4.1.3; 4.3.2; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 7.4; 11.3].
- 13.7 ISO/IEC 27701:2025 - Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5. Addressed by clauses [4.2.4; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 7.1; 7.5].
- 13.8 ISO/IEC 27701:2025 - Annex A.1.5.2; Annex A.1.5.3; Annex A.1.5.4; Annex A.1.5.5. Addressed by clauses [4.7.3; 4.7.4; 4.7.5; 7.7].
- 13.9 ISO/IEC 27701:2025 - Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7. Addressed by clauses [4.1.5; 4.3.5; 4.5.5; 4.7.1; 4.7.2; 5.7; 6.3; 7.6].
- 13.10 ISO/IEC 27701:2025 - Annex A.2.3.2; Annex A.2.5.2; Annex A.2.5.3; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6. Addressed by clauses [4.3.5; 4.5.5; 4.7.1; 4.7.2; 4.7.4; 4.7.5; 7.6; 7.7].
- 13.11 ISO/IEC 27701:2025 - Annex A.3.14; Annex A.3.25. Addressed by clauses [4.4.4; 4.6.1; 4.6.3; 4.8.1; 5.4; 7.5; 7.8; 10.2].
- 13.12 GDPR - Article 4(4); Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(d); Article 5(2). Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.3.1; 4.4.1; 4.4.2; 4.4.5; 4.8.1; 8.1].
- 13.13 GDPR - Article 6; Article 9; Article 10. Addressed by clauses [4.1.2; 4.2.4; 4.4.3; 4.7.3; 7.1].
- 13.14 GDPR - Article 12; Article 13; Article 14; Article 15. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.5.2; 4.5.3; 7.3; 11.3].
- 13.15 GDPR - Article 16; Article 17; Article 18; Article 21; Article 22. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 7.4].
- 13.16 GDPR - Article 24; Article 25; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39. Addressed by clauses [4.1.4; 4.1.5; 4.2.1; 4.2.2; 4.2.5; 4.4.4; 4.7.1; 4.8.2; 5.3; 6.2; 6.4; 7.2].
- 13.17 GDPR - Article 44. Addressed by clauses [4.7.4; 7.7; 8.4].
- 13.18 ISO/IEC 29100:2020 - Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.7. Addressed by clauses [4.1.2; 4.2.4; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.7.5].
- 13.19 ISO/IEC 29100:2020 - Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12. Addressed by clauses [4.3.1; 4.3.2; 4.5.1; 4.5.2; 4.6.3; 4.8.1; 4.8.2; 8.5; 10.1].
- 13.20 ISO/IEC 29134:2020 - Clause 5.1; Clause 6.2; Clause 6.3. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.5; 4.6.4; 6.4; 7.2; 9.2].
- 13.21 ISO/IEC 29151:2022 - Annex A.4; Annex A.5; Annex A.7; Annex A.8; Annex A.10. Addressed by clauses [4.3.1; 4.3.2; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.5.2; 4.5.4; 4.7.5].