					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: PII08					Titolo del documento: **Politica di privacy by design e privacy by default**							
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**

Allineamento a standard e normative applicabili

Standard / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 6.1.2; Clause 6.1.3	Both	Supporting	Collegamento con valutazione del rischio privacy e relativo trattamento
ISO/IEC 27701:2025	Clause 6.3; Clause 8.1	Both	Primary	Modifiche pianificate e controllo operativo
ISO/IEC 27701:2025	Clause 7.5	Both	Supporting	Evidenze documentate della progettazione privacy
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.1.2.6; Annex A.1.2.9	Controller	Supporting	Finalità, trigger PIA e registrazioni
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3	Controller	Primary	Limitazione della raccolta e del trattamento
ISO/IEC 27701:2025	Annex A.1.4.4; Annex A.1.4.5	Controller	Supporting	Obiettivi di accuratezza e minimizzazione
ISO/IEC 27701:2025	Annex A.1.4.6; Annex A.1.4.7	Controller	Supporting	Progettazione di de-identificazione, cancellazione e file temporanei
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6; Annex A.2.2.7	Processor	Supporting	Accordo con il cliente, supporto e registrazioni del responsabile del trattamento
ISO/IEC 27701:2025	Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4	Processor	Supporting	Capacità progettuali del responsabile del trattamento
ISO/IEC 27701:2025	Annex A.3.27; Annex A.3.29	Both	Supporting	Ciclo di vita dello sviluppo e principi ingegneristici
GDPR	Article 5(1)(b); Article 5(1)(c); Article 5(2)	Controller	Supporting	Limitazione della finalità, minimizzazione e responsabilizzazione
GDPR	Article 24	Controller	Supporting	Misure del titolare del trattamento

GDPR	Article 25	Controller	Primary	Protezione dei dati fin dalla progettazione e per impostazione predefinita
GDPR	Article 28	Both	Supporting	Istruzioni e assistenza del responsabile del trattamento
GDPR	Article 30	Both	Supporting	Registrazioni dei trattamenti
GDPR	Article 35	Controller	Supporting	Collegamento con il trigger DPIA
ISO/IEC 29100:2020	Clause 4.7	Both	Supporting	Controlli privacy fin dalla progettazione
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Primary	Finalità, raccolta, minimizzazione e limitazione dell’uso
ISO/IEC 29100:2020	Clause 5.7; Clause 5.10; Clause 5.12	Both	Supporting	Accuratezza, responsabilizzazione e conformità
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.8	Both	Primary	Principi e controlli di protezione delle PII

1. Ambito di applicazione

1.1 La presente politica definisce i requisiti per integrare la privacy by design e la privacy by default nelle attività di trattamento di PII nuove e modificate, nei progetti, prodotti, servizi, sistemi, applicazioni, integrazioni, attività di approvvigionamento e modifiche dei processi aziendali nell'ambito di applicazione del PIMS.

1.2 La presente politica si applica ai contesti di titolare del trattamento, contitolare del trattamento, responsabile del trattamento e sub-responsabile. Gli obblighi del responsabile del trattamento e del sub-responsabile si applicano quando l'organizzazione progetta, configura, modifica o gestisce trattamenti per conto di un cliente, titolare del trattamento o responsabile del trattamento a monte, sulla base di istruzioni documentate.

1.3 La presente politica copre:

1.3.1 i requisiti privacy all'avvio del progetto;

1.3.2 i controlli di progettazione relativi a finalità, minimizzazione dei dati e impostazioni predefinite;

1.3.3 il riesame della progettazione privacy prima della messa in esercizio;

1.3.4 il riesame della progettazione privacy attivato da modifiche;

1.3.5 le verifiche di approvvigionamento relative alla protezione dei dati fin dalla progettazione;

1.3.6 il collegamento con il rischio privacy, lo screening DPIA e le evidenze delle azioni correttive.

1.4 La presente politica non sostituisce:

1.4.1 PII03 per inventario dei trattamenti, finalità, base giuridica e registrazioni ROPA;

1.4.2 PII04 per il contenuto e la pubblicazione dell'informativa privacy;

1.4.3 PII05 per i controlli sul consenso e sulle preferenze;

1.4.4 PII06 per la gestione dei diritti degli interessati;

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

1.4.6 PII09 per i controlli di raccolta, uso, divulgazione e condivisione;

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

1.4.8 PII11 per l'operatività di accuratezza e qualità;

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

1.4.10 PII13 per i meccanismi di trasferimento internazionale;

1.4.11 PII14 per la sicurezza delle PII e l'operatività del controllo degli accessi;

1.4.12 PII18 per il monitoraggio, l'audit, le azioni correttive e la governance del miglioramento a livello dell'intero PIMS.

2. Finalità

2.1 La finalità della presente politica è assicurare che i requisiti privacy siano identificati, applicati e comprovati prima che il trattamento di PII inizi o subisca modifiche sostanziali, e che sistemi e processi siano configurati per impostazione predefinita in modo da limitare la raccolta, l'uso, l'esposizione, la dipendenza dalla conservazione, la dipendenza dalla divulgazione e l'identificabilità delle PII a quanto necessario per la finalità documentata.

3. Obiettivi

3.1 Gli obiettivi della presente politica sono:

3.1.1 integrare i requisiti privacy nelle decisioni di avvio progetto, progettazione, approvvigionamento, modifica e messa in esercizio;

3.1.2 assicurare che le progettazioni dei trattamenti di PII siano collegate alle finalità documentate e alle registrazioni dei trattamenti REG02;

3.1.3 applicare la minimizzazione dei dati e impostazioni predefinite a tutela della privacy prima dell'avvio del trattamento;

3.1.4 assicurare l'attivazione dello screening del rischio privacy e della DPIA senza duplicare la metodologia PII07;

3.1.5 assicurare che i requisiti di progettazione relativi ad approvvigionamento e responsabili del trattamento siano registrati senza duplicare la governance del ciclo di vita PII12;

3.1.6 assicurare che le questioni progettuali non risolte siano sottoposte a escalation tramite REG12;

3.1.7 mantenere evidenze di progettazione disponibili in sede di audit in REG02, REG04, REG08 e REG12.

4. Dichiarazioni della politica

4.1 Avvio del progetto e requisiti privacy

4.1.1 [Both] Il Process Owner / Business Owner DEVE registrare una voce di progettazione privacy in REG04 prima di avviare qualsiasi progetto, prodotto, servizio, sistema, applicazione, integrazione o modifica di processo aziendale che coinvolga PII.

4.1.2 [Both] Il Process Owner / Business Owner DEVE collegare ogni voce di progettazione privacy in REG04 a un'attività di trattamento REG02 esistente o in bozza prima dell'approvazione dei requisiti funzionali.

4.1.3 [Controller] Il Privacy Lead / PIMS Manager DEVE registrare in REG04 i requisiti del titolare del trattamento relativi alla protezione dei dati fin dalla progettazione prima dell'approvazione della progettazione funzionale del titolare del trattamento.

4.1.4 [Processor] Il Vendor / Procurement Owner DEVE registrare in REG08 le istruzioni di progettazione privacy del cliente e i vincoli contrattuali di progettazione prima dell'approvazione della progettazione del servizio del responsabile del trattamento o di una modifica sostanziale del servizio.

4.1.5 [Conditional] Il Data Protection Officer / Privacy Advisor DEVE registrare il parere in REG04 prima dell'approvazione di una progettazione di PII ad alto rischio, innovativa, sensibile, automatizzata, su larga scala o modificata in modo sostanziale.

4.1.6 [Both] L'Information Security Lead DEVE registrare in REG04 le dipendenze dai controlli di sicurezza delle PII che supportano la progettazione privacy prima dell'approvazione dell'architettura.

4.2 Minimizzazione dei dati e progettazione privacy predefinita

4.2.1 [Controller] Il Process Owner / Business Owner DEVE documentare le categorie minime di PII, le categorie di interessati, le fonti e le finalità in REG02 e REG04 prima dell'approvazione della progettazione della raccolta o dell'importazione.

4.2.2 [Both] Il System Owner / Application Owner DEVE configurare le impostazioni predefinite del trattamento al livello minimo di raccolta e trattamento di PII necessario per la finalità documentata e registrare le evidenze in REG04 prima della messa in esercizio.

4.2.3 [Controller] Il Process Owner / Business Owner DEVE documentare i campi PII facoltativi, le scelte di trattamento facoltative e le impostazioni disattivate per impostazione predefinita in REG02 e REG04 prima dell'approvazione dell'interfaccia utente, del modulo o del workflow.

4.2.4 [Both] Il System Owner / Application Owner DEVE documentare in REG04 le impostazioni predefinite di esposizione privacy per viste, report, esportazioni, interfacce e workflow automatizzati prima della messa in esercizio.

4.2.5 [Both] Il Process Owner / Business Owner DEVE documentare in REG04 la fattibilità di de-identificazione, pseudonimizzazione, aggregazione o trattamento non identificabile prima di approvare PII identificabili per test, analisi, reportistica o uso operativo secondario.

4.2.6 [Both] Il System Owner / Application Owner DEVE documentare in REG04 la gestione degli artifact temporanei di PII, inclusi file temporanei, cache, log o registrazioni di staging, prima della messa in esercizio.

4.2.7 [Both] Il Process Owner / Business Owner DEVE indirizzare i requisiti di progettazione di competenza di PII10, PII11, PII13 o PII14 al relativo percorso di evidenza della politica in REG04 entro cinque giorni lavorativi dall'identificazione della dipendenza.

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

9. Eccezioni

9.1 Eccezioni di progettazione privacy

9.1.1 [Both] Il Process Owner / Business Owner DEVE richiedere un'eccezione di progettazione privacy in REG12 prima di approvare una progettazione o una modifica che non possa soddisfare un requisito di progettazione privacy applicabile.

9.1.2 [Both] Il Privacy Lead / PIMS Manager DEVE valutare in REG12 l'impatto, i controlli compensativi e la scadenza di ciascuna eccezione di progettazione privacy entro cinque giorni lavorativi dalla richiesta.

9.1.3 [Conditional] Il Data Protection Officer / Privacy Advisor DEVE registrare il parere in REG12 prima dell'approvazione di un'eccezione di progettazione privacy che coinvolga trattamenti ad alto rischio, sensibili, automatizzati, su larga scala, contestati o giuridicamente rilevanti.

9.1.4 [All] Top Management DEVE approvare in REG12 un'eccezione di progettazione privacy che incida su trattamenti ad alto impatto, ambito di certificazione, rischio maggiore non risolto o obbligo legale prima che l'eccezione produca effetti.

9.1.5 [Both] Il Privacy Lead / PIMS Manager DEVE impostare in REG12, per ciascuna eccezione di progettazione privacy approvata, una data di scadenza non superiore a 90 giorni prima dell'approvazione.

9.1.6 [Both] Il Privacy Lead / PIMS Manager DEVE chiudere o rivalutare ciascuna eccezione di progettazione privacy in REG12 entro cinque giorni lavorativi dalla scadenza.

10. Applicazione della politica

10.1 Applicazione della politica e gestione delle non conformità

10.1.1 [Both] Il Privacy Lead / PIMS Manager DEVE registrare in REG12 il riesame mancante della progettazione privacy, l'assenza di evidenze di minimizzazione, il fallimento non risolto delle impostazioni predefinite o la messa in esercizio non autorizzata come non conformità entro cinque giorni lavorativi dall'identificazione.

10.1.2 [Both] Il System Owner / Application Owner DEVE impedire la messa in esercizio di un sistema di trattamento di PII quando il riesame della progettazione privacy REG04 è incompleto e registrare la decisione in REG12 prima della messa in esercizio.

10.1.3 [Both] Il Vendor / Procurement Owner DEVE impedire l'onboarding del fornitore o la firma del contratto quando le evidenze di progettazione privacy REG08 richieste sono assenti e registrare la decisione in REG12 prima dell'onboarding o della firma.

10.1.4 [Both] Il Process Owner / Business Owner DEVE sospendere l'uso di una progettazione di trattamento di PII nuova o modificata finché il riesame REG04, gli aggiornamenti REG02 e le eccezioni REG12 richieste non siano completati.

10.1.5 [All] Top Management DEVE richiedere un'azione correttiva in REG12 entro 10 giorni lavorativi per fallimenti ripetuti, prolungati o ad alto impatto della progettazione privacy.

10.1.6 [All] L'Internal Audit / Compliance Reviewer DEVE verificare l'efficacia delle azioni correttive per le non conformità di progettazione privacy in REG12 al successivo audit PIMS programmato o entro 60 giorni dalla chiusura, se precedente.

11. Riesame e manutenzione

11.1 Riesame della politica e dei controlli di progettazione

11.1.1 [All] Il Privacy Lead / PIMS Manager DEVE riesaminare la presente politica in REG12 con cadenza annuale ed entro 30 giorni da una modifica sostanziale legale, di trattamento, tecnologica, dell'ambito di certificazione o dei controlli PIMS.

11.1.2 [Both] Il Process Owner / Business Owner DEVE riesaminare annualmente le attività di trattamento REG02 attive per individuare modifiche alle dipendenze della progettazione privacy ed entro 30 giorni da una modifica sostanziale del trattamento.

11.1.3 [Both] Il System Owner / Application Owner DEVE riesaminare le evidenze di configurazione privacy predefinita in REG04 con cadenza annuale ed entro 30 giorni da una modifica sostanziale del sistema.

11.1.4 [Both] Il Vendor / Procurement Owner DEVE riesaminare in REG08 gli obblighi di progettazione privacy relativi a fornitori, responsabili del trattamento, sub-responsabili e terze parti prima del rinnovo ed entro 30 giorni da una modifica sostanziale del rapporto.

11.1.5 [Conditional] Il Data Protection Officer / Privacy Advisor DEVE riesaminare l'impatto privacy delle modifiche sostanziali alla politica in REG12 prima dell'approvazione.

11.1.6 [All] Top Management DEVE approvare le modifiche sostanziali alla presente politica in REG12 prima della pubblicazione.

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 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 PII09 - Politica di raccolta, uso, divulgazione e condivisione delle PII

12.9 PII10 - Politica di conservazione, cancellazione e smaltimento delle PII

12.10 PII11 - Politica di accuratezza e qualità delle PII

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

12.12 PII13 - Politica sui trasferimenti internazionali di PII

12.13 PII14 - Politica di sicurezza delle PII e controllo degli accessi

12.14 PII17 - Politica di gestione delle informazioni documentate e delle evidenze del PIMS

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

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 li supportano.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.1.2; Clause 6.1.3** - Mappate allo screening del rischio privacy, al collegamento delle azioni di trattamento, all'analisi delle dipendenze progettuali, all'escalation e alle azioni correttive senza duplicare l'intera metodologia di valutazione del rischio privacy e DPIA. Addressed by clauses [4.1.5; 4.3.1; 4.3.2; 4.3.4; 4.5.5; 5.1.3; 7.1.7].

13.2.2 **Clause 6.3; Clause 8.1** - Mappate alle modifiche privacy pianificate, all'avvio del progetto, al riesame operativo della progettazione privacy, al controllo della messa in esercizio e al riesame delle modifiche sostanziali. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.3.3; 4.3.5; 4.5.1; 4.5.3; 4.5.4; 4.5.6; 7.1.2; 7.1.5; 10.1.2].

13.2.3 **Clause 7.5** - Mappata alle evidenze documentate di progettazione privacy conservate in REG02, REG04, REG08 e REG12. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.2.3; 4.4.1; 4.4.2; 4.4.3; 5.1.2; 5.1.5; 5.1.6; 5.1.7; 7.1.1; 7.1.3; 7.1.4].

13.2.4 **Clause 9.1; Clause 10.2** - Mappate alle metriche di progettazione privacy, al campionamento delle evidenze, alla registrazione delle non conformità, alle azioni correttive e alla verifica dell'efficacia. Addressed by clauses [4.3.6; 4.4.5; 4.5.5; 6.1.1; 6.1.2; 6.1.4; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 10.1.1; 10.1.5; 10.1.6].

13.2.5 **Annex A.1.2.2; Annex A.1.2.6; Annex A.1.2.9** - Mappati alla documentazione delle finalità del trattamento, alle registrazioni dei trattamenti, al collegamento della progettazione privacy e ai trigger di screening del rischio privacy o della DPIA per il trattamento del titolare del trattamento. Addressed by clauses [4.1.2; 4.2.1; 4.3.1; 4.4.2; 4.5.2; 5.1.5; 7.1.3; 11.1.2].

13.2.6 **Annex A.1.4.2; Annex A.1.4.3** - Mappati alla limitazione della raccolta e del trattamento di PII tramite requisiti di dati minimi basati sulla finalità, trattamento facoltativo disattivato per impostazione predefinita e impostazioni predefinite minime di trattamento. Addressed by clauses [4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.5.4; 7.1.5; 11.1.3].

13.2.7 **Annex A.1.4.4; Annex A.1.4.5** - Mappati all'instradamento delle dipendenze di accuratezza, agli obiettivi di minimizzazione, alla fattibilità della de-identificazione e alle evidenze di progettazione per minimizzare le PII identificabili. Addressed by clauses [4.2.5; 4.2.7; 4.3.2; 4.5.2; 7.1.3; 11.1.2].

13.2.8 **Annex A.1.4.6; Annex A.1.4.7** - Mappati all'identificazione in fase di progettazione della de-identificazione, della dipendenza dalla cancellazione, degli artifact temporanei di PII e dell'instradamento ai controlli del ciclo di vita senza duplicare l'esecuzione della conservazione o dello smaltimento. Addressed by clauses [4.2.5; 4.2.6; 4.2.7; 4.3.3; 4.5.4; 7.1.5; 11.1.3].

13.2.9 **Annex A.2.2.2; Annex A.2.2.6; Annex A.2.2.7** - Mappati alle istruzioni del cliente al responsabile del trattamento, alle informazioni di supporto al cliente, alle registrazioni di progettazione del responsabile del trattamento e alle modifiche della progettazione del servizio autorizzate dal cliente. Addressed by clauses [4.1.4; 4.4.1; 4.4.3; 4.4.6; 5.1.7; 7.1.4; 11.1.4].

13.2.10 **Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4** - Mappati alle capacità progettuali del responsabile del trattamento per file temporanei, dipendenza da restituzione o smaltimento e dipendenza dai controlli di trasmissione, registrate come evidenze di progettazione senza duplicare le procedure operative di cancellazione o dei controlli di sicurezza. Addressed by clauses [4.2.6; 4.2.7; 4.4.3; 4.4.4; 4.4.6; 7.1.4; 7.1.6; 11.1.4].

13.2.11 **Annex A.3.27; Annex A.3.29** - Mappati ai requisiti privacy nel ciclo di vita dello sviluppo, ai principi ingegneristici, ai checkpoint di protezione delle PII e alle evidenze di configurazione privacy predefinita. Addressed by clauses [4.1.6; 4.3.3; 4.3.4; 4.4.4; 4.5.1; 4.5.4; 5.1.4; 5.1.6; 7.1.5; 7.1.6; 10.1.2; 11.1.3].

13.3 GDPR

13.3.1 **Article 5(1)(b); Article 5(1)(c); Article 5(2)** - Mappati alla limitazione della finalità, alla progettazione con PII minime, al collegamento con le registrazioni dei trattamenti, alla minimizzazione predefinita, alle evidenze e alla responsabilizzazione. Addressed by clauses [4.1.2; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.4.2; 4.5.2; 5.1.5; 8.1.1; 10.1.1].

13.3.2 **Article 24** - Mappato alle misure del titolare del trattamento, al riesame di governance, all'approvazione delle eccezioni, alle azioni correttive e alla manutenzione della politica per l'applicazione della protezione dei dati fin dalla progettazione. Addressed by clauses [4.1.3; 4.5.6; 5.1.1; 6.1.2; 9.1.2; 9.1.4; 10.1.5; 11.1.6].

13.3.3 **Article 25** - Mappato all'avvio del progetto, ai requisiti privacy in fase di progettazione, alle impostazioni privacy predefinite, alla minimizzazione, alle verifiche di progettazione in approvvigionamento, al riesame della messa in esercizio e al riesame attivato da modifiche. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.5; 4.4.1; 4.5.1; 4.5.3; 4.5.4; 10.1.2].

13.3.4 **Article 28** - Mappato alle istruzioni del responsabile del trattamento, al supporto alla progettazione da parte del responsabile del trattamento, alle evidenze di progettazione privacy dei fornitori e alle modifiche di progettazione autorizzate dal cliente. Addressed by clauses [4.1.4; 4.4.1; 4.4.3; 4.4.5; 4.4.6; 5.1.7; 7.1.4; 10.1.3; 11.1.4].

13.3.5 **Article 30** - Mappato al collegamento con le registrazioni dei trattamenti, agli aggiornamenti REG02, alle dipendenze progettuali delle attività di trattamento e alle evidenze delle registrazioni dei trattamenti. Addressed by clauses [4.1.2; 4.2.1; 4.4.2; 4.5.2; 5.1.5; 7.1.3; 11.1.2].

13.3.6 **Article 35** - Mappato ai trigger di screening del rischio privacy e della DPIA in fase di progettazione, al parere sui rischi elevati e alle verifiche post-implementazione senza duplicare la metodologia DPIA. Addressed by clauses [4.1.5; 4.3.1; 4.3.6; 5.1.3; 6.1.3; 9.1.3].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.7** - Mappata all'identificazione dei controlli privacy nella fase di progettazione, al collegamento con il rischio privacy e alle evidenze di progettazione per l'applicazione dei controlli. Addressed by clauses [4.1.1; 4.1.3; 4.1.5; 4.3.1; 4.3.2; 4.3.3; 4.3.5; 4.5.1].

13.4.2 **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, all'uso limitato e alle impostazioni predefinite di trattamento. Addressed by clauses [4.1.2; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.4.2; 4.5.2].

13.4.3 **Clause 5.7; Clause 5.10; Clause 5.12** - Mappate all'instradamento delle dipendenze di accuratezza, alle evidenze di responsabilizzazione, al monitoraggio della progettazione privacy, all'audit e alle azioni correttive. Addressed by clauses [4.2.7; 4.3.6; 4.5.5; 6.1.1; 6.1.4; 8.1.1; 8.1.2; 10.1.1; 10.1.6].

13.5 ISO/IEC 29151:2022

13.5.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.8** - Mappati alla legittimità della finalità, alla limitazione della raccolta, alla minimizzazione dei dati, alla limitazione dell'uso e della divulgazione, alla dipendenza dalla conservazione, alla gestione dei file temporanei e ai controlli di progettazione relativi alla dipendenza dall'accuratezza. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7; 4.4.2; 4.5.2; 4.5.4; 7.1.3; 7.1.5].