					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: PII03					Titolo del documento: **Politica sull'inventario dei trattamenti PII e sulla base giuridica**							
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 4.1	Both	Supporting	Determinazione del ruolo PIMS per le attività di trattamento
ISO/IEC 27701:2025	Clause 6.1.2	Both	Supporting	Collegamento al trigger della valutazione del rischio privacy
ISO/IEC 27701:2025	Clause 6.1.3	Both	Supporting	Collegamento all'applicabilità dei controlli e alla SoA
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Informazioni documentate dell'inventario dei trattamenti
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Pianificazione operativa e controllo per le registrazioni dei trattamenti
ISO/IEC 27701:2025	Clause 8.2	Both	Supporting	Collegamento alla valutazione operativa del rischio privacy
ISO/IEC 27701:2025	Clause 9.1	Both	Supporting	Monitoraggio e misurazione dell'inventario
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Non conformità dell'inventario e azione correttiva
ISO/IEC 27701:2025	Annex A.1.2.2	Controller	Primary	Identificazione delle finalità del titolare del trattamento
ISO/IEC 27701:2025	Annex A.1.2.3	Controller	Primary	Identificazione della base giuridica del titolare del trattamento
ISO/IEC 27701:2025	Annex A.1.2.6	Controller	Supporting	Collegamento allo screening DPIA
ISO/IEC 27701:2025	Annex A.1.2.8	Joint Controller	Supporting	Registrazioni delle responsabilità del trattamento in contitolarità
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Registrazioni del titolare del

				trattamento relative al trattamento di PII
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Primary	Registrazioni dell'accordo con il cliente e delle istruzioni del responsabile del trattamento
ISO/IEC 27701:2025	Annex A.2.2.3	Processor	Primary	Allineamento delle finalità del responsabile del trattamento alle istruzioni del cliente
ISO/IEC 27701:2025	Annex A.2.2.7	Processor	Supporting	Registrazioni del responsabile del trattamento relative al trattamento di PII
GDPR	Article 5(1)(a)	Controller	Supporting	Collegamento a liceità, correttezza e trasparenza
GDPR	Article 5(1)(b)	Controller	Supporting	Limitazione della finalità
GDPR	Article 5(1)(c)	Controller	Supporting	Minimizzazione dei dati
GDPR	Article 5(1)(e)	Controller	Supporting	Collegamento alla limitazione della conservazione
GDPR	Article 5(2)	Controller	Supporting	Evidenze di responsabilizzazione
GDPR	Article 6	Controller	Primary	Liceità del trattamento
GDPR	Article 9	Conditional	Supporting	Condizione per il trattamento di categorie particolari di dati
GDPR	Article 10	Conditional	Supporting	Condizione per dati relativi a condanne penali e reati
GDPR	Article 24	Controller	Supporting	Responsabilità e misure del titolare del trattamento
GDPR	Article 26	Joint Controller	Supporting	Registrazioni degli accordi di contitolarità
GDPR	Article 28	Both	Supporting	Registrazioni delle istruzioni e degli

				accordi con il responsabile del trattamento
GDPR	Article 30	Both	Primary	Registri delle attività di trattamento
GDPR	Article 35	Controller	Supporting	Collegamento allo screening DPIA
ISO/IEC 29100:2020	Clause 5.3	Both	Supporting	Legittimità e specificazione della finalità
ISO/IEC 29100:2020	Clause 5.4	Both	Supporting	Limitazione della raccolta
ISO/IEC 29100:2020	Clause 5.5	Both	Supporting	Minimizzazione dei dati
ISO/IEC 29100:2020	Clause 5.6	Both	Supporting	Limitazione di uso, conservazione e comunicazione
ISO/IEC 29100:2020	Clause 5.10	Both	Supporting	Responsabilizzazione
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7	Controller	Supporting	Controlli per la protezione di PII relativi a finalità, raccolta, minimizzazione, uso, conservazione e comunicazione
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2	Both	Supporting	Collegamento ai benefici e ai trigger della PIA

1. Ambito di applicazione

1.1 La presente politica definisce i requisiti per mantenere l'inventario dei trattamenti PII / ROPA e documentare la base giuridica, le finalità del trattamento, i ruoli di trattamento, le categorie di PII, le categorie di interessati, i destinatari, i riferimenti di conservazione, i riferimenti di trasferimento, le istruzioni del responsabile del trattamento, le registrazioni dei contitolari del trattamento e il collegamento allo screening del rischio privacy.

1.2 La presente politica si applica a:

1.2.1 tutte le attività di trattamento di PII comprese nell'ambito di applicazione del PIMS;

1.2.2 il trattamento svolto come titolare del trattamento, contitolare del trattamento, responsabile del trattamento o sub-responsabile;

1.2.3 il trattamento svolto da processi aziendali, sistemi, applicazioni, fornitori, responsabili del trattamento, sub-responsabili e destinatari della condivisione dei dati;

1.2.4 nuovi trattamenti, trattamenti modificati in modo sostanziale e trattamenti cessati;

1.2.5 le evidenze mantenute in REG02 e le evidenze di supporto in REG01, REG03, REG04, REG05, REG07, REG08, REG09 e REG12.

1.3 La presente politica non sostituisce i controlli dettagliati sulle informative privacy, i controlli sul consenso, la metodologia DPIA, l'esecuzione della conservazione, la selezione del meccanismo di trasferimento internazionale, i controlli contrattuali dei responsabili del trattamento, i controlli di sicurezza PII o i controlli sulle informazioni documentate. Tali requisiti sono definiti nelle politiche correlate elencate nella Sezione 12.

1.4 Ai fini della presente politica, per registrazione dell'inventario dei trattamenti si intende una voce REG02 che descrive una distinta attività di trattamento di PII, inclusi finalità, ruolo, proprietario, categorie di PII, categorie di interessati, base giuridica o riferimento all'istruzione del cliente, sistemi, destinatari, riferimento di conservazione, riferimento di trasferimento, stato del rischio privacy e stato del riesame.

1.5 Ai fini della presente politica, per modifica sostanziale del trattamento si intende qualsiasi modifica della finalità del trattamento, della base giuridica, del ruolo PIMS, della categoria di PII, della categoria di interessati, del destinatario, del sistema, del fornitore, del sub-responsabile, del luogo di trattamento, del trasferimento, della regola di conservazione, della classificazione di sicurezza, dell'informativa privacy, della dipendenza dal consenso, dello stato DPIA, dell'istruzione del cliente o dell'ambito della certificazione.

2. Finalità

2.1 La finalità della presente politica è garantire che l'organizzazione possa identificare, documentare, giustificare, riesaminare e dimostrare le attività di trattamento di PII comprese nell'ambito di applicazione del PIMS.

2.2 La presente politica consente all'organizzazione di mantenere un inventario dei trattamenti di PII completo, aggiornato e idoneo a dimostrare la conformità in sede di audit, a supporto del trattamento lecito, della responsabilizzazione, delle informative privacy, della gestione del consenso, della valutazione del rischio privacy, dello screening DPIA, della conservazione, della governance dei trasferimenti, della governance dei responsabili del trattamento e del monitoraggio del PIMS.

3. Obiettivi

3.1 Gli obiettivi della presente politica sono:

3.1.1 istituire REG02 come oggetto di evidenza autorevole per l'inventario dei trattamenti PII e il ROPA;

3.1.2 garantire che ogni attività di trattamento di PII abbia un proprietario responsabile;

3.1.3 distinguere le registrazioni di trattamento come titolare del trattamento, contitolare del trattamento, responsabile del trattamento e sub-responsabile;

3.1.4 documentare le specifiche finalità del trattamento prima dell'avvio del trattamento;

3.1.5 documentare la base giuridica del trattamento effettuato come titolare del trattamento prima dell'avvio del trattamento;

3.1.6 documentare le istruzioni del cliente per il trattamento effettuato come responsabile del trattamento e sub-responsabile prima dell'avvio del trattamento;

3.1.7 documentare le categorie di PII, le categorie di interessati, i destinatari, i riferimenti di conservazione, i riferimenti di trasferimento, i sistemi e i rapporti con i fornitori;

3.1.8 collegare le registrazioni dell'inventario alle informative privacy, al consenso, alla DPIA, al rischio, ai fornitori, ai trasferimenti, ai controlli e alle evidenze di audit, ove applicabile;

3.1.9 garantire che le registrazioni dell'inventario dei trattamenti siano riesaminate, aggiornate e corrette quando il trattamento cambia;

3.1.10 evitare la creazione di registri separati della base giuridica o dell'inventario dei trattamenti al di fuori di REG02.

4. Dichiarazioni della politica

4.1 Baseline dell'inventario dei trattamenti

4.1.1 [Both] Il Process Owner / Business Owner deve creare una registrazione dell'inventario dei trattamenti in REG02 prima dell'avvio di qualsiasi nuova attività di trattamento di PII.

4.1.2 [Both] Il Process Owner / Business Owner deve registrare i campi REG02 richiesti per ogni attività di trattamento prima dell'avvio dell'attività.

4.1.3 [Both] Il Privacy Lead / PIMS Manager deve approvare l'insieme dei campi REG02 richiesti in REG12 prima dell'operatività iniziale del PIMS e successivamente con cadenza annuale.

4.1.4 [Both] Il Process Owner / Business Owner deve classificare in REG02 il ruolo PIMS dell'organizzazione per ogni attività di trattamento prima dell'avvio dell'attività.

4.1.5 [Both] Il System Owner / Application Owner deve collegare ogni sistema o applicazione che tratta PII alla relativa attività di trattamento REG02 prima della messa in esercizio del sistema.

4.1.6 [Both] Il Vendor / Procurement Owner deve collegare ogni rapporto con responsabile del trattamento, sub-responsabile, condivisione con terze parti o contitolare del trattamento in REG08 alla relativa attività di trattamento REG02 prima dell'approvazione dell'accordo o dell'onboarding.

4.2 Registrazioni della finalità e della base giuridica del titolare del trattamento

4.2.1 [Controller] Il Process Owner / Business Owner deve documentare in REG02 la specifica finalità del trattamento prima che PII siano raccolte, utilizzate, comunicate o altrimenti trattate.

4.2.2 [Controller] Il Privacy Lead / PIMS Manager deve validare la base giuridica registrata in REG02 prima dell'avvio del trattamento come titolare del trattamento e prima che abbia effetto qualsiasi modifica della finalità.

4.2.3 [Controller] Il Data Protection Officer / Privacy Advisor deve registrare un parere in REG12 prima dell'approvazione di una nuova base giuridica per trattamenti ad alto rischio, categorie particolari di PII, dati relativi a condanne penali o reati, oppure trattamenti come titolare del trattamento modificati in modo sostanziale.

4.2.4 [Controller] Il Process Owner / Business Owner deve collegare REG02 a REG05 prima che il trattamento come titolare del trattamento si basi sul consenso quale base giuridica.

4.2.5 [Controller] Il Process Owner / Business Owner deve registrare in REG04 il riferimento alla valutazione dell'interesse legittimo prima che il trattamento come titolare del trattamento si basi su interessi legittimi.

4.2.6 [Conditional] Il Process Owner / Business Owner deve registrare in REG02 la condizione per il trattamento di categorie particolari prima di trattare categorie particolari di PII.

4.2.7 [Conditional] Il Privacy Lead / PIMS Manager deve registrare in REG02 la base di autorizzazione per dati relativi a condanne penali o reati prima di trattare tali dati.

4.2.8 [Controller] Il Process Owner / Business Owner deve documentare in REG02 e REG04 la compatibilità della finalità e lo screening del rischio privacy prima di utilizzare PII per una nuova finalità non precedentemente registrata.

[... 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 relative all'inventario dei trattamenti e alla base giuridica

9.1.1 [All] Il Process Owner / Business Owner deve richiedere un'eccezione in REG12 prima di svolgere un'attività di trattamento di PII senza un campo REG02 richiesto, una registrazione della base giuridica, un riferimento all'istruzione del cliente o uno stato di riesame.

9.1.2 [All] Il Privacy Lead / PIMS Manager deve valutare in REG12 l'impatto privacy, di certificazione e operativo di ciascuna eccezione all'inventario dei trattamenti entro 10 giorni lavorativi dalla richiesta.

9.1.3 [All] Il Data Protection Officer / Privacy Advisor deve registrare un parere in REG12 prima dell'approvazione di qualsiasi eccezione che riguardi base giuridica, categorie particolari di PII, dati relativi a condanne penali o reati, trattamenti ad alto rischio, collegamento a trasferimenti internazionali o limitazione delle istruzioni del cliente.

9.1.4 [All] Top Management deve approvare in REG12 le eccezioni all'inventario dei trattamenti che superano 30 giorni, incidono su trattamenti ad alto rischio o incidono sull'ambito della certificazione prima che l'eccezione abbia effetto.

9.1.5 [All] Il Privacy Lead / PIMS Manager deve impostare in REG12 una data di scadenza non superiore a 90 giorni per ciascuna eccezione approvata dell'inventario dei trattamenti prima dell'approvazione.

9.1.6 [All] Il Process Owner / Business Owner deve chiudere o rivalutare ciascuna eccezione all'inventario dei trattamenti in REG12 entro cinque giorni lavorativi dalla scadenza.

10. Applicazione della politica

10.1 Applicazione in materia di inventario dei trattamenti e base giuridica

10.1.1 [All] Il Privacy Lead / PIMS Manager deve registrare in REG12 come non conformità le evidenze dell'inventario dei trattamenti REG02 mancanti, inesatte, obsolete o non approvate entro cinque giorni lavorativi dall'identificazione.

10.1.2 [Controller] Il Process Owner / Business Owner deve sospendere i nuovi trattamenti come titolare del trattamento quando l'evidenza richiesta della finalità o della base giuridica manca da REG02 prima del lancio.

10.1.3 [Processor] Il Process Owner / Business Owner deve sospendere i nuovi trattamenti come responsabile del trattamento quando l'evidenza richiesta delle istruzioni del cliente manca da REG02 o REG08 prima dell'onboarding del servizio.

10.1.4 [Both] Il System Owner / Application Owner deve bloccare la messa in esercizio del sistema per il trattamento di PII quando il collegamento richiesto all'inventario REG02 manca prima dell'approvazione della messa in esercizio.

10.1.5 [Both] Il Vendor / Procurement Owner deve bloccare l'onboarding di fornitori, responsabili del trattamento, sub-responsabili, destinatari terzi o contitolari del trattamento quando le evidenze richieste di collegamento REG02 e REG08 mancano prima dell'approvazione dell'accordo.

10.1.6 [All] Top Management deve riesaminare in REG12, durante il riesame della direzione, le non conformità maggiori non risolte relative all'inventario dei trattamenti o alla base giuridica.

10.1.7 [All] L'Internal Audit / Compliance Reviewer deve verificare in REG12 l'efficacia delle azioni correttive per le non conformità relative all'inventario dei trattamenti al successivo audit pianificato o entro 60 giorni dalla chiusura, a seconda di quale evento si verifichi per primo.

11. Riesame e mantenimento

11.1 Riesame e mantenimento della politica

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 dei requisiti relativi a inventario dei trattamenti, base giuridica, istruzioni del responsabile del trattamento, ROPA o certificazione.

11.1.2 [All] Il Privacy Lead / PIMS Manager deve riesaminare in REG12 i requisiti minimi dei campi REG02 con cadenza annuale ed entro 30 giorni da una modifica sostanziale legale, normativa, contrattuale o del trattamento.

11.1.3 [All] Il Data Protection Officer / Privacy Advisor deve riesaminare in REG12 le modifiche alla presente politica rilevanti per la privacy prima dell'approvazione.

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

11.1.5 [All] Il Privacy Lead / PIMS Manager deve aggiornare REG03 e REG04 entro 15 giorni lavorativi dalle modifiche approvate alla politica che alterano l'applicabilità dei controlli o i requisiti di screening del rischio privacy.

11.1.6 [All] Il Privacy Lead / PIMS Manager deve registrare in REG11 la comunicazione delle modifiche approvate alla presente politica entro 30 giorni dalla pubblicazione.

12. Politiche correlate

12.1 La presente politica è supportata dalle seguenti politiche correlate:

12.2 PII01 - Politica del sistema di gestione delle informazioni sulla privacy

12.3 PII02 - Politica su ruoli, responsabilità e responsabilizzazione in materia di privacy

12.4 PII04 - Politica sulle informative privacy e sulla trasparenza

12.5 PII05 - Politica di gestione del consenso e delle preferenze

12.6 PII07 - Politica di valutazione del rischio privacy e DPIA

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

12.8 PII09 - Politica di raccolta, uso, comunicazione 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 e controllo degli accessi alle PII

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 4.1** - Mappata alla determinazione del ruolo PIMS dell'organizzazione per ciascuna attività di trattamento e alla distinzione tra contesti di titolare del trattamento, contitolare del trattamento, responsabile del trattamento e sub-responsabile. Addressed by clauses [4.1.4; 4.3.1; 4.3.4; 4.3.5].

13.2.2 **Clause 6.1.2** - Mappata al collegamento del trigger della valutazione del rischio privacy per attività di trattamento di PII nuove e modificate in modo sostanziale. Addressed by clauses [4.2.8; 4.5.2; 4.5.3].

13.2.3 **Clause 6.1.3** - Mappata al collegamento delle attività di trattamento all'applicabilità dei controlli e alle evidenze della Dichiarazione di Applicabilità del PIMS. Addressed by clauses [4.5.4; 7.1.5; 11.1.5].

13.2.4 **Clause 7.5** - Mappata al mantenimento delle registrazioni dell'inventario dei trattamenti, della base giuridica, delle istruzioni del responsabile del trattamento, dei riesami, delle eccezioni e delle azioni correttive come informazioni documentate controllate. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.2; 4.3.1; 4.4.1; 4.5.1; 7.1.1; 7.1.3; 9.1.1; 10.1.1].

13.2.5 **Clause 8.1** - Mappata alla pianificazione operativa e controllo per creare, validare, aggiornare, riesaminare e ritirare le registrazioni dell'inventario dei trattamenti prima che il trattamento inizi o cambi. Addressed by clauses [4.1.1; 4.1.5; 4.1.6; 4.5.1; 4.5.6; 7.1.2; 7.1.6; 7.1.7; 7.1.8].

13.2.6 **Clause 8.2** - Mappata al collegamento della valutazione operativa del rischio privacy dalle registrazioni dell'inventario dei trattamenti e dai trigger di modifica sostanziale del trattamento. Addressed by clauses [4.2.8; 4.5.2; 4.5.3; 8.1.5].

13.2.7 **Clause 9.1** - Mappata al monitoraggio e alla misurazione della completezza dell'inventario dei trattamenti, della validazione della base giuridica, del collegamento alle istruzioni, dello stato dei riesami, del collegamento allo screening DPIA e delle eccezioni di riconciliazione. Addressed by clauses [4.5.4; 4.5.5; 6.1.1; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 8.1.7; 8.1.8].

13.2.8 **Clause 10.2** - Mappata alla gestione delle non conformità, eccezioni, azioni correttive, applicazione della politica e verifica dell'efficacia relative all'inventario e alla base giuridica. Addressed by clauses [9.1.1; 9.1.2; 9.1.4; 9.1.6; 10.1.1; 10.1.6; 10.1.7].

13.2.9 **Annex A.1.2.2** - Mappata all'identificazione e alla documentazione delle finalità del trattamento come titolare del trattamento prima che PII siano raccolte, utilizzate, comunicate o altrimenti trattate. Addressed by clauses [4.1.2; 4.2.1; 4.2.8; 4.3.5].

13.2.10 **Annex A.1.2.3** - Mappata alla determinazione, documentazione, validazione e dimostrazione della base giuridica per il trattamento come titolare del trattamento. Addressed by clauses [4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7].

13.2.11 **Annex A.1.2.6** - Mappata allo screening delle attività di trattamento nuove e modificate in modo sostanziale come titolare del trattamento per determinare la necessità di DPIA. Addressed by clauses [4.5.2; 4.5.3; 8.1.5].

13.2.12 **Annex A.1.2.8** - Mappata alla registrazione delle finalità del trattamento in contitolarità e dei riferimenti alla ripartizione delle responsabilità. Addressed by clauses [4.1.6; 4.3.5; 10.1.5].

13.2.13 **Annex A.1.2.9** - Mappata al mantenimento delle registrazioni del titolare del trattamento relative al trattamento di PII, inclusi finalità, categorie, destinatari, riferimenti di conservazione, trasferimenti, base giuridica, screening del rischio, proprietario, stato ed evidenze di riesame.

Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.4.6; 4.5.1; 4.5.6; 7.1.2; 7.1.8].

13.2.14 **Annex A.2.2.2** - Mappata all'accordo con il cliente del responsabile del trattamento e alle evidenze delle istruzioni documentate, inclusi oggetto, durata, finalità, categorie di PII e categorie di interessati. Addressed by clauses [4.3.1; 4.3.2; 5.1.7; 10.1.3].

13.2.15 **Annex A.2.2.3** - Mappata alla garanzia che le finalità del trattamento svolto dal responsabile del trattamento restino allineate alle istruzioni documentate del cliente. Addressed by clauses [4.3.1; 4.3.3; 4.3.4; 10.1.3].

13.2.16 **Annex A.2.2.7** - Mappata al mantenimento delle registrazioni del responsabile del trattamento relative al trattamento di PII per conto dei clienti. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 8.1.3].

13.3 GDPR

13.3.1 **Article 5(1)(a)** - Mappata alla finalità del trattamento come titolare del trattamento, alla validazione della base giuridica e alle evidenze di responsabilizzazione prima dell'avvio del trattamento. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.8].

13.3.2 **Article 5(1)(b)** - Mappata alla specificazione della finalità, alla valutazione della compatibilità della finalità e alla prevenzione di trattamenti per nuove finalità non documentate. Addressed by clauses [4.2.1; 4.2.8; 4.3.3].

13.3.3 **Article 5(1)(c)** - Mappata alla registrazione delle categorie di PII, delle categorie di interessati e dei dati di origine prima del trattamento, a supporto del riesame della minimizzazione. Addressed by clauses [4.1.2; 4.4.1; 4.4.6].

13.3.4 **Article 5(1)(e)** - Mappata alla registrazione della regola di conservazione o del riferimento di conservazione per ciascuna attività di trattamento. Addressed by clauses [4.4.4; 8.1.6].

13.3.5 **Article 5(2)** - Mappata alle evidenze di responsabilizzazione per inventario dei trattamenti, validazione della base giuridica, riesame, riconciliazione, campionamento di audit e azione correttiva. Addressed by clauses [4.1.1; 4.2.2; 4.5.4; 4.5.5; 6.1.2; 10.1.1; 10.1.7].

13.3.6 Article 6 - Mappata alla documentazione e validazione della base giuridica per il trattamento come titolare del trattamento, inclusi il collegamento al consenso, il riferimento alla valutazione dell'interesse legittimo e la compatibilità della finalità. Addressed by clauses [4.2.2; 4.2.4; 4.2.5; 4.2.8].

13.3.7 Article 9 - Mappata alla registrazione della condizione per il trattamento di categorie particolari e del parere privacy prima del trattamento di categorie particolari di PII. Addressed by clauses [4.2.3; 4.2.6; 9.1.3].

13.3.8 **Article 10** - Mappata alla registrazione della base di autorizzazione per dati relativi a condanne penali o reati prima del trattamento. Addressed by clauses [4.2.3; 4.2.7; 9.1.3].

13.3.9 **Article 24** - Mappata alla governance, al riesame, alla responsabilizzazione e alla supervisione della direzione del titolare del trattamento sulle registrazioni dell'inventario dei trattamenti e della base giuridica. Addressed by clauses [4.2.2; 5.1.1; 6.1.2; 10.1.6; 11.1.4].

13.3.10 **Article 26** - Mappata alle evidenze della finalità del trattamento in contitolarità e della ripartizione delle responsabilità. Addressed by clauses [4.1.6; 4.3.5; 10.1.5].

13.3.11 **Article 28** - Mappata ai controlli relativi a istruzioni, accordi, collegamento dei rapporti e onboarding di responsabili del trattamento e sub-responsabili. Addressed by clauses [4.1.6; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 5.1.7; 7.1.7; 10.1.3; 10.1.5].

13.3.12 **Article 30** - Mappata alle registrazioni delle attività di trattamento del titolare del trattamento e del responsabile del trattamento, inclusi finalità del trattamento, categorie di PII, categorie di interessati, destinatari, trasferimenti, riferimenti di conservazione e registrazioni

delle istruzioni del cliente. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.3.1; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.5.1; 4.5.6; 7.1.2].

13.3.13 **Article 35** - Mappata al collegamento allo screening DPIA per attività di trattamento nuove, modificate in modo sostanziale o ad alto rischio come titolare del trattamento. Addressed by clauses [4.2.8; 4.5.2; 4.5.3; 8.1.5].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.3** - Mappata alla legittimità della finalità, alla specificazione della finalità, al collegamento alla base giuridica e alle evidenze di compatibilità della finalità. Addressed by clauses [4.2.1; 4.2.2; 4.2.8; 4.3.1; 4.3.3].

13.4.2 **Clause 5.4** - Mappata alla limitazione della raccolta mediante documentazione delle categorie di PII, delle categorie di interessati, delle fonti e della giustificazione prima dell'avvio del trattamento. Addressed by clauses [4.1.2; 4.4.1; 4.4.6].

13.4.3 **Clause 5.5** - Mappata alla minimizzazione dei dati mediante requisiti dei campi dell'inventario, documentazione delle categorie, documentazione dei destinatari e riesame delle registrazioni di trattamento correnti. Addressed by clauses [4.1.2; 4.4.1; 4.4.2; 4.5.4; 8.1.6].

13.4.4 **Clause 5.6** - Mappata alla limitazione di uso, conservazione, comunicazione e trasferimento mediante finalità documentate, categorie di destinatari, riferimenti di conservazione, collegamento ai trasferimenti e controlli sulle modifiche di finalità. Addressed by clauses [4.2.1; 4.2.8; 4.4.2; 4.4.4; 4.4.5].

13.4.5 **Clause 5.10** - Mappata alla responsabilizzazione mediante titolarità, governance dell'inventario, riesame, riconciliazione, campionamento di audit, gestione delle eccezioni ed evidenze di azione correttiva. Addressed by clauses [4.1.1; 4.1.3; 4.5.4; 4.5.5; 5.1.5; 6.1.1; 8.1.1; 10.1.1].

13.5 ISO/IEC 29151:2022

13.5.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7** - Mappata ai controlli di protezione delle PII per legittimità della finalità, limitazione della raccolta, minimizzazione dei dati e limitazione di uso, conservazione e comunicazione. Addressed by clauses [4.2.1; 4.2.2; 4.4.1; 4.4.2; 4.4.4; 4.4.6; 4.5.4; 8.1.6].

13.6 ISO/IEC 29134:2020

13.6.1 **Clause 5.1; Clause 6.2** - Mappata all'uso delle modifiche dell'inventario dei trattamenti per attivare la valutazione del rischio privacy e lo screening DPIA prima che proceda un trattamento nuovo o modificato in modo sostanziale. Addressed by clauses [4.2.8; 4.5.2; 4.5.3; 8.1.5].