					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: PII19					Titolo del documento: **Politica sulla privacy dei dipendenti**							
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 7.5; Clause 8.1	Both	Primary	Evidenze sulla privacy dei dipendenti e controllo operativo
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitoraggio, non conformità e azione correttiva
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.8; Annex A.1.2.9	Controller	Primary	Finalità HR, collegamento alla base giuridica, trigger DPIA, responsabilità congiunta e registrazioni
ISO/IEC 27701:2025	Annex A.1.2.7; Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7	Both	Supporting	Contratti con responsabili del trattamento HR, istruzioni, assistenza e registrazioni
ISO/IEC 27701:2025	Annex A.1.3.2; Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10; Annex A.1.3.11	Controller	Supporting	Obblighi dei dipendenti, diritti e instradamento del processo decisionale automatizzato
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	Collegamento a raccolta, trattamento, minimizzazione e conservazione
ISO/IEC 27701:2025	Annex A.1.5.4; Annex A.1.5.5; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Both	Supporting	Registrazioni delle comunicazioni e gestione delle comunicazioni giuridicamente vincolanti
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Protezione delle registrazioni HR ed evidenze di logging
GDPR	Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2)	Controller	Primary	Principi di privacy dei dipendenti e responsabilizzazione
GDPR	Article 6; Article 9; Article 10	Controller	Supporting	Liceità, categorie particolari e dati di

				background screening
GDPR	Article 12; Article 13; Article 14	Controller	Primary	Trasparenza e informative per i dipendenti
GDPR	Article 15; Article 16; Article 17; Article 18; Article 21; Article 22	Controller	Supporting	Diritti dei dipendenti e instradamento del processo decisionale automatizzato
GDPR	Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39	Both	Supporting	Governance, contitolari del trattamento, 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, uso, 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 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10	Controller	Supporting	Finalità PII, raccolta, minimizzazione, conservazione e partecipazione dell'interessato
ISO/IEC 29151:2022	Clause 7.1.2; Clause 7.1.3; Clause 7.2.4; Clause 7.3.2	Controller	Supporting	Controlli del ciclo di vita del personale a protezione delle PII
ISO/IEC 29151:2022	Clause 15.1.2; Clause 15.2.2; Clause 15.2.3	Both	Supporting	Valutazione dei responsabili del trattamento HR, monitoraggio e controllo delle modifiche
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2	Controller	Supporting	Collegamento tra rischio privacy HR e trigger DPIA
ISO/IEC 27002:2022	Controls 5.34; 6.1; 6.2; 6.5; 6.6	Both	Supporting	Protezione delle PII e ciclo di vita della sicurezza delle

				informazioni del personale
ISO/IEC 27002:2022	Controls 8.15; 8.16	Both	Supporting	Attività di logging e monitoraggio

1. Ambito di applicazione

1.1 La presente politica definisce i requisiti di privacy dei dipendenti per la raccolta, l'uso, la comunicazione, il collegamento alla conservazione, l'informativa, la gestione dei diritti, il monitoraggio, il supporto dei responsabili del trattamento e la gestione delle evidenze delle PII dei dipendenti all'interno del Sistema di gestione delle informazioni sulla privacy.

1.2 Ai fini della presente politica, per “PII dei dipendenti” si intendono le PII relative a dipendenti, candidati, ex dipendenti, collaboratori esterni, personale temporaneo, tirocinanti, personale distaccato e altri partecipanti alla forza lavoro quando l'organizzazione tratta le loro PII per finalità connesse a forza lavoro, selezione, rapporto di lavoro, incarico, retribuzione, benefit, sicurezza, conformità, amministrazione del luogo di lavoro o finalità aziendali correlate.

1.3 La presente politica si applica ai contesti di titolare del trattamento e contitolare del trattamento in cui l'organizzazione determina le finalità e i mezzi del trattamento delle PII dei dipendenti.

1.4 La presente politica si applica inoltre ai contesti di responsabile del trattamento e sub-responsabile nei quali l'organizzazione tratta PII dei dipendenti per conto di un cliente, di un responsabile del trattamento a monte o di un altro titolare del trattamento sulla base di istruzioni documentate.

1.5 La presente politica copre:

1.5.1 raccolta dei dati dei dipendenti;

1.5.2 finalità di trattamento HR;

1.5.3 informative privacy per i dipendenti;

1.5.4 gestione dei diritti dei dipendenti;

1.5.5 collegamento alla conservazione;

1.5.6 monitoraggio dei dipendenti;

1.5.7 comunicazione interna;

1.5.8 controlli relativi a responsabili del trattamento HR, payroll, HRIS, benefit, background screening e servizi HR esternalizzati, ove applicabile;

1.5.9 incidenti relativi alle PII dei dipendenti, non conformità, azioni correttive ed evidenze di miglioramento.

1.6 La presente politica non istituisce un registro privacy HR separato, un registro privacy dei dipendenti, un registro dei trattamenti HR, un registro del monitoraggio dei dipendenti, un registro del background screening, un registro dei fornitori HR, un registro dei diritti dei dipendenti o un registro degli incidenti dei dipendenti. Le evidenze relative al trattamento dei dipendenti sono registrate in REG02, REG04, REG06, REG07, REG08, REG10 e REG12.

1.7 La presente politica non fornisce consulenza in materia di diritto del lavoro, consulenza in materia di relazioni sindacali, commenti giuridici sul comitato aziendale, contenuti di procedure disciplinari, contenuti di procedure operative di payroll o modelli di documenti di lavoro specifici per giurisdizione.

1.8 La presente politica non duplica:

1.8.1 governance del PIMS in PII01;

1.8.2 responsabilità dei ruoli in PII02;

1.8.3 inventario dei trattamenti e titolarità della base giuridica in PII03;

1.8.4 governance dei contenuti dell'informativa privacy in PII04;

1.8.5 operatività del consenso e delle preferenze in PII05;

1.8.6 workflow dei diritti dell'interessato in PII06;

1.8.7 metodologia di rischio privacy e DPIA in PII07;

1.8.8 gate di privacy by design in PII08;

1.8.9 regole di baseline per raccolta, uso, comunicazione e condivisione in PII09;

1.8.10 esecuzione della conservazione, cancellazione e smaltimento in PII10;

1.8.11 governance di accuratezza e qualità in PII11;

1.8.12 governance del ciclo di vita di responsabili del trattamento, sub-responsabili e terze parti in PII12;

1.8.13 controlli sugli strumenti di trasferimento internazionale in PII13;

1.8.14 applicazione della sicurezza e del controllo degli accessi in PII14;

1.8.15 gestione degli incidenti e delle violazioni in PII15;

1.8.16 gestione della formazione e della sensibilizzazione in PII16;

1.8.17 controllo delle informazioni documentate in PII17;

1.8.18 governance del monitoraggio, dell'audit e del miglioramento del PIMS in PII18;

1.8.19 controlli relativi all'AI e al processo decisionale automatizzato in PII21, quando tale politica opzionale è inclusa.

2. Finalità

2.1 La finalità della presente politica è assicurare che le PII dei dipendenti siano trattate solo per finalità relative alla forza lavoro documentate, approvate, trasparenti, proporzionate e soggette a responsabilizzazione, e che le evidenze sulla privacy dei dipendenti siano mantenute nei registri canonici del PIMS senza creare un livello separato di evidenze privacy HR.

2.2 La presente politica supporta una gestione coerente del trattamento dei dipendenti collegando le attività di trattamento dei dipendenti a REG02, le informative privacy dei dipendenti a REG07, le richieste di esercizio dei diritti dei dipendenti a REG06, il rischio privacy HR e i trigger DPIA a REG04, i responsabili del trattamento HR e i fornitori di payroll o HRIS a REG08, gli incidenti relativi alle PII dei dipendenti a REG10, e le eccezioni, le non conformità, le azioni correttive e le evidenze di monitoraggio a REG12.

3. Obiettivi

3.1 Gli obiettivi della presente politica sono:

3.1.1 mantenere in REG02 le evidenze dell'inventario dei trattamenti dei dipendenti;

3.1.2 documentare fonti di raccolta, categorie di PII, finalità, sistemi, destinatari e collegamento alla conservazione relativi ai dipendenti;

3.1.3 mantenere in REG07 le evidenze delle informative privacy dei dipendenti;

3.1.4 instradare il rischio privacy dei dipendenti e i trigger DPIA tramite REG04;

3.1.5 instradare le richieste di esercizio dei diritti dei dipendenti tramite REG06;

3.1.6 mantenere in REG08 le evidenze relative a responsabili del trattamento HR, payroll, HRIS, benefit, background screening e servizi HR esternalizzati;

3.1.7 assicurare che il monitoraggio dei dipendenti sia documentato, proporzionato, riesaminato e sottoposto a escalation tramite REG04 e REG12 ove applicabile;

3.1.8 instradare gli incidenti sospetti relativi alle PII dei dipendenti tramite REG10;

3.1.9 registrare in REG12 le eccezioni privacy dei dipendenti, le non conformità, le azioni correttive e le azioni di miglioramento;

3.1.10 evitare consulenza in materia di diritto del lavoro e commenti giuridici sul comitato aziendale all'interno delle clausole operative;

3.1.11 evitare registri, ruoli, moduli, dashboard o elementi di evidenza specifici per HR duplicati.

4. Dichiarazioni della politica

4.1 Inventario dei trattamenti dei dipendenti e finalità di trattamento HR

4.1.1 [Controller] Il Process Owner / Business Owner deve registrare ciascuna attività di trattamento dei dipendenti in REG02 prima che le PII dei dipendenti siano raccolte, generate, importate, usate o comunicate.

4.1.2 [Controller] Il Process Owner / Business Owner deve documentare in REG02 le categorie di PII dei dipendenti, la popolazione di dipendenti, la fonte di raccolta, la finalità del trattamento, il sistema, la categoria di destinatari interni, la categoria di destinatari esterni e il collegamento alla conservazione prima che l'attività di trattamento sia approvata.

4.1.3 [Controller] Il Privacy Lead / PIMS Manager deve riesaminare in REG02 ogni attività di trattamento dei dipendenti nuova o modificata in modo sostanziale prima che l'attività di trattamento sia approvata per l'operatività.

4.1.4 [Conditional] Il Data Protection Officer / Privacy Advisor deve registrare la consulenza privacy in REG04 prima dell'approvazione del trattamento dei dipendenti che coinvolge PII appartenenti a categorie particolari, dati relativi a reati, background screening, dati di medicina del lavoro, biometria, dati di localizzazione, monitoraggio dei dipendenti o trattamenti che possono incidere in modo sostanziale su un dipendente.

4.1.5 [Processor] Il Privacy Lead / PIMS Manager deve registrare in REG08 l'istruzione del cliente, la finalità del servizio, le categorie di PII dei dipendenti del cliente e il collegamento al ruolo di responsabile del trattamento prima di trattare PII dei dipendenti del cliente come servizio esternalizzato di HR, payroll, benefit, HRIS, screening o supporto alla forza lavoro.

4.1.6 [Joint Controller] Il Privacy Lead / PIMS Manager deve registrare in REG08 l'allocazione delle responsabilità del contitolare del trattamento per il trattamento delle PII dei dipendenti prima dell'avvio dell'attività congiunta di trattamento dei dipendenti.

4.2 Raccolta dei dati dei dipendenti e informative privacy dei dipendenti

4.2.1 [Controller] Il Process Owner / Business Owner deve limitare la raccolta delle PII dei dipendenti alle categorie documentate in REG02 prima dell'avvio della raccolta per selezione, onboarding, amministrazione del rapporto di lavoro, amministrazione dei benefit, operatività del payroll, screening, monitoraggio o offboarding.

4.2.2 [Controller] Il Process Owner / Business Owner deve registrare in REG02 la fonte delle PII dei dipendenti raccolte da terze parti prima che la fonte di raccolta di terza parte sia utilizzata.

4.2.3 [Controller] Il Privacy Lead / PIMS Manager deve mantenere in REG07 una registrazione dell'informativa privacy dei dipendenti prima che le PII dei dipendenti siano raccolte direttamente o indirettamente per una finalità nuova o modificata in modo sostanziale.

4.2.4 [Controller] Il Process Owner / Business Owner deve confermare che l'informativa privacy dei dipendenti corrente registrata in REG07 sia disponibile prima della raccolta per selezione, della raccolta per onboarding, dell'attivazione del monitoraggio, dell'iscrizione ai benefit, del background screening o di una modifica sostanziale del trattamento dei dipendenti.

4.2.5 [Conditional] Il Data Protection Officer / Privacy Advisor deve riesaminare la registrazione dell'informativa privacy dei dipendenti in REG07 prima della pubblicazione quando l'informativa copre monitoraggio dei dipendenti, background screening, PII appartenenti a categorie particolari, dati relativi a reati, processo decisionale automatizzato o una finalità di trattamento dei dipendenti modificata in modo sostanziale.

4.2.6 [Processor] Il Vendor / Procurement Owner deve registrare in REG08 le responsabilità relative ai canali di raccolta rivolti ai dipendenti prima che un servizio HR, payroll, HRIS, benefit, screening o HR esternalizzato gestito da un responsabile del trattamento raccolga PII dei dipendenti per conto di un cliente.

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

9. Eccezioni

9.1.1 [All] Il Process Owner / Business Owner deve registrare una richiesta di eccezione in REG12 prima di discostarsi da qualsiasi requisito della presente politica.

9.1.2 [Conditional] Il Data Protection Officer / Privacy Advisor deve registrare la consulenza in REG12 prima dell'approvazione di un'eccezione che incide sul monitoraggio dei dipendenti, sulla gestione dei diritti dei dipendenti, sul background screening, su PII appartenenti a categorie particolari, dati relativi a reati o trattamento dei dipendenti ad alto impatto.

9.1.3 [Conditional] Top Management deve approvare le eccezioni privacy dei dipendenti in REG12 prima dell'attivazione quando l'eccezione incide su trattamento dei dipendenti ad alto rischio, monitoraggio dei dipendenti, comunicazione esterna, affidamento a un responsabile del trattamento o azione correttiva non risolta.

9.1.4 [All] Il Privacy Lead / PIMS Manager deve assegnare in REG12 a ciascuna eccezione privacy dei dipendenti una data di scadenza non superiore a 90 giorni prima che l'eccezione sia attivata.

9.1.5 [All] Il Privacy Lead / PIMS Manager deve riesaminare ciascuna eccezione privacy dei dipendenti in REG12 entro cinque giorni lavorativi prima della scadenza.

9.1.6 [All] Il Privacy Lead / PIMS Manager deve chiudere o sottoporre a escalation ciascuna eccezione privacy dei dipendenti scaduta in REG12 entro cinque giorni lavorativi dalla scadenza.

10. Applicazione della politica

10.1.1 [All] Il Privacy Lead / PIMS Manager deve registrare una non conformità in REG12 entro cinque giorni lavorativi quando il trattamento delle PII dei dipendenti non dispone delle evidenze REG02, REG07, REG08, REG04 o REG06 richieste.

10.1.2 [Conditional] L'Incident Response Coordinator deve registrare in REG10 sospetti accessi non autorizzati, comunicazioni, perdite o compromissioni di PII dei dipendenti entro un giorno lavorativo dall'identificazione.

10.1.3 [Controller] Il Privacy Lead / PIMS Manager deve impedire l'approvazione di un nuovo monitoraggio dei dipendenti in REG12 quando mancano le evidenze REG02, REG04 o REG07 richieste.

10.1.4 [Both] Il Vendor / Procurement Owner deve sospendere in REG08 nuove comunicazioni di PII dei dipendenti a un fornitore HR quando mancano le evidenze richieste relative a responsabile del trattamento, sub-responsabile, istruzioni o assistenza.

10.1.5 [All] Top Management deve riesaminare le non conformità privacy dei dipendenti ripetute in REG12 quando la stessa categoria si verifica due o più volte in un periodo mobile di 12 mesi.

10.1.6 [All] L'Internal Audit / Compliance Reviewer deve verificare le evidenze di chiusura in REG12 prima di chiudere risultanze dell'audit che coinvolgono trattamento privacy dei dipendenti, informative ai dipendenti, monitoraggio dei dipendenti, diritti dei dipendenti o fornitori HR.

11. Riesame e manutenzione

11.1.1 [All] Il Privacy Lead / PIMS Manager deve riesaminare la presente politica in REG12 almeno annualmente.

11.1.2 [Conditional] Il Privacy Lead / PIMS Manager deve riesaminare la presente politica in REG12 entro 30 giorni da una modifica sostanziale al trattamento dei dipendenti, al monitoraggio dei dipendenti, ai sistemi HR, agli accordi di payroll, ai fornitori HRIS, ai fornitori di benefit, ai fornitori di background screening o ai servizi HR esternalizzati.

11.1.3 [Conditional] Il Data Protection Officer / Privacy Advisor deve riesaminare le modifiche sostanziali proposte alla presente politica in REG12 prima dell'approvazione di Top Management.

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

11.1.5 [All] Il Privacy Lead / PIMS Manager deve aggiornare REG02, REG07 o REG08 entro 15 giorni lavorativi dopo che una modifica approvata della politica incide sulle registrazioni dei trattamenti dei dipendenti, sulle informative privacy dei dipendenti o sulle evidenze dei fornitori HR.

11.1.6 [All] L'Internal Audit / Compliance Reviewer deve registrare in REG12 le osservazioni sull'efficacia del riesame della presente politica durante il ciclo di audit interno del PIMS programmato.

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

12.5 PII04 - Politica sull'informativa privacy e sulla trasparenza

12.6 PII05 - Politica di gestione del consenso e delle preferenze

12.7 PII06 - Politica di gestione dei diritti dell'interessato relativi alle PII

12.8 PII07 - Politica di valutazione del rischio privacy e DPIA

12.9 PII08 - Politica di privacy by design e by default

12.10 PII09 - Politica su raccolta, uso, comunicazione e condivisione delle PII

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

12.12 PII11 - Politica di accuratezza e qualità delle PII

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

12.14 PII13 - Politica sui trasferimenti internazionali di PII

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

12.16 PII15 - Politica di gestione degli incidenti e delle violazioni relativi alle PII

12.17 PII16 - Politica di formazione, sensibilizzazione e competenza in materia di privacy

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

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

12.20 PII21 - Politica privacy su AI e processo decisionale automatizzato, ove inclusa nell'ambito del rilascio opzionale aggiuntivo

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 7.5; Clause 8.1** - Mappato a evidenze documentate sulla privacy dei dipendenti, gate di approvazione operativa, registrazioni dei responsabili del trattamento HR, informative ai dipendenti, registrazioni di monitoraggio, gestione delle eccezioni ed evidenze di attuazione. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.3; 4.3.1; 4.4.1; 4.5.1; 4.7.1; 7.1.1; 7.1.3].

13.2.2 **Clause 9.1; Clause 10.2** - Mappato a monitoraggio della privacy dei dipendenti, metriche, evidenze di audit, campionamento del monitoraggio dei dipendenti, gestione delle non conformità, azione correttiva e miglioramento. Addressed by clauses [4.3.6; 4.4.5; 4.5.5; 4.6.7; 8.1.1; 8.1.4; 8.1.7; 10.1.1; 10.1.5].

13.2.3 **Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.8; Annex A.1.2.9** - Mappato a finalità di trattamento dei dipendenti, collegamento alla base giuridica, instradamento di rischio privacy e DPIA, allocazione tra contitolari del trattamento e registrazioni dei trattamenti in REG02 e REG04. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.6; 4.2.2; 4.6.1; 4.6.2].

13.2.4 **Annex A.1.2.7; Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7** - Mappato a contratti con responsabili del trattamento HR, istruzioni documentate, trattamento delle PII dei dipendenti del cliente, assistenza del responsabile del trattamento e registrazioni del responsabile del trattamento in REG08. Addressed by clauses [4.1.5; 4.2.6; 4.4.4; 4.5.4; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5].

13.2.5 **Annex A.1.3.2; Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10; Annex A.1.3.11** - Mappato alla gestione dei diritti dei dipendenti, alla consulenza su diritti complessi e all'instradamento del processo decisionale automatizzato o del trattamento ad alto impatto tramite REG06 e REG04. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.3].

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** - Mappato alla limitazione della raccolta dei dipendenti, all'uso interno approvato, alla minimizzazione, al collegamento alla conservazione e all'instradamento delle eccezioni di conservazione. Addressed by clauses [4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.6.1].

13.2.7 **Annex A.1.5.4; Annex A.1.5.5; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6** - Mappato a comunicazioni esterne di PII dei dipendenti, registrazioni di condivisione dei dati, autorizzazione alla comunicazione da parte del responsabile del trattamento e instradamento degli incidenti relativi alla comunicazione. Addressed by clauses [4.3.4; 4.3.5; 4.3.6; 4.7.6].

13.2.8 **Annex A.3.14; Annex A.3.25** - Mappato alla protezione delle registrazioni privacy dei dipendenti, alle evidenze dei log di monitoraggio dei dipendenti e a sospetto uso improprio o compromissione dei dati di monitoraggio dei dipendenti. Addressed by clauses [4.6.4; 4.6.6; 4.6.7; 7.1.2].

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)** - Mappato a trattamento delle PII dei dipendenti lecito, corretto, trasparente, limitato alla finalità, minimizzato, collegato alla conservazione e soggetto a responsabilizzazione. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.3.1; 4.3.3; 4.4.1; 4.4.5].

13.3.2 **Article 6; Article 9; Article 10** - Mappato al collegamento alla base giuridica, all'instradamento delle PII dei dipendenti appartenenti a categorie particolari, all'instradamento delle PII sensibili relative a medicina del lavoro e rapporto di lavoro e all'instradamento di dati relativi a reati o background screening. Addressed by clauses [4.1.2; 4.1.3; 4.1.4; 4.2.2; 4.7.3].

13.3.3 **Article 12; Article 13; Article 14** - Mappato a trasparenza verso i dipendenti, registrazioni delle informative privacy dei dipendenti, trigger di informativa per raccolta diretta e indiretta ed evidenze di informativa sul monitoraggio. Addressed by clauses [4.2.3; 4.2.4; 4.2.5; 4.6.5].

13.3.4 **Article 15; Article 16; Article 17; Article 18; Article 21; Article 22** - Mappato a instradamento dei diritti dei dipendenti, evidenze delle richieste, consulenza su richieste complesse e instradamento del processo decisionale automatizzato. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.3].

13.3.5 **Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39** - Mappato a governance del titolare del trattamento, allocazione tra contitolari del trattamento,

governance dei responsabili del trattamento HR, registrazioni dei trattamenti, gestione sicura, instradamento DPIA e coinvolgimento della consulenza privacy. Addressed by clauses [4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.3.4; 4.3.5; 4.6.2; 4.6.3; 4.6.6; 4.7.1; 4.7.6].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6** - Mappato alla specificazione delle finalità dei dipendenti, alla limitazione della raccolta, alla minimizzazione, alla limitazione dell'uso, alla limitazione della conservazione e alla limitazione della comunicazione. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.4.1; 4.4.2; 4.6.1].

13.4.2 **Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12** - Mappato a trasparenza, partecipazione dei dipendenti, supporto ai diritti dei dipendenti, responsabilizzazione, sicurezza delle informazioni ed evidenze di conformità privacy. Addressed by clauses [4.2.3; 4.2.4; 4.5.1; 4.5.2; 4.5.5; 4.6.4; 4.6.6; 4.6.7; 4.7.6].

13.5 ISO/IEC 29151:2022

13.5.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10** - Mappato a registrazioni delle finalità PII, controlli di raccolta, minimizzazione, collegamento alla conservazione, limitazione della comunicazione e partecipazione o supporto all'accesso dei dipendenti. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.3.1; 4.3.4; 4.4.1; 4.4.2; 4.5.1; 4.5.4].

13.5.2 **Clause 7.1.2; Clause 7.1.3; Clause 7.2.4; Clause 7.3.2** - Mappato a controlli del ciclo di vita del personale a protezione delle PII relativi a screening, condizioni, collegamento all'applicazione in caso di violazione privacy e riesame della conservazione in caso di cessazione o modifica del rapporto di lavoro. Addressed by clauses [4.1.4; 4.2.2; 4.4.2; 4.4.5; 10.1.1; 10.1.5].

13.5.3 **Clause 15.1.2; Clause 15.2.2; Clause 15.2.3** - Mappato a valutazione dei responsabili del trattamento HR, monitoraggio dei responsabili del trattamento HR, riesame dei fornitori HR ed evidenze di modifica del servizio in REG08. Addressed by clauses [4.4.4; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 4.7.6].

13.6 ISO/IEC 29134:2020

13.6.1 **Clause 5.1; Clause 6.2** - Mappato ai benefici della valutazione d'impatto sulla privacy e alla determinazione del rischio privacy HR o del trigger DPIA per il monitoraggio dei dipendenti e il trattamento HR ad alto impatto senza duplicare il metodo DPIA. Addressed by clauses [4.1.4; 4.3.3; 4.6.2; 4.6.3].

13.7 ISO/IEC 27002:2022

13.7.1 Controls 5.34; 6.1; 6.2; 6.5; 6.6 - Mappato a protezione delle PII, screening, condizioni del personale, responsabilità dopo modifiche del rapporto di lavoro e aspettative di riservatezza quali controlli del ciclo di vita del personale a supporto delle PII. Addressed by clauses [4.1.4; 4.2.2; 4.4.2; 4.4.4; 4.7.2; 4.7.3].

13.7.2 Controls 8.15; 8.16 - Mappato a log di monitoraggio dei dipendenti, attività di monitoraggio, limitazione della finalità dei log e riesame delle evidenze di monitoraggio. Addressed by clauses [4.6.1; 4.6.2; 4.6.4; 4.6.6; 4.6.7].