PERITO GROUP S.R.L.
Via Fonti, snc
84036 Sala Consilina (SA)
Email info@peritogroup.it
PEC peritogroup@arubapec.it
Tel. 0975-520350
P. IVA 04321630651

POLITICA DI PROTEZIONE DEI DATI PERSONALI DEI DIPENDENTI

Codice:	02.2
Revisione:	0.1
Data di revisione:	18/01/2023
Redatta da:	Avv. Nicola Pellegrino
Approvata da:	Dott. Giuseppe Perito
Livello di Riservatezza:	NORMALE possono accedere a questo documenti solo coloro che sono autorizzati secondo le regole definite per l'accesso

Cronologia delle revisioni

Data	Revisione	Creata da	Descrizione della modifica
18/01/2023	0.1	Avv. Nicola Pellegrino	redazione documento base

Sommario

1. CAMPO D'APPLICAZIONE, SCOPO E DESTINATARI 3

2. DOCUMENTI DI RIFERIMENTO 3

3. DEFINIZIONI 4

3.1. DATO PERSONALE 4
3.2. DATI PERSONALI SENSIBILI 4
3.3. TRATTAMENTO 4
3.4. CONTROLLORE DEI DATI: 5

4. PRINCIPI GENERALI PER IL TRATTAMENTO DEI DATI PERSONALI DEI DIPENDENTI 5

4.1. LICEITÀ, CORRETTEZZA E TRASPARENZA 5
4.2. LIMITAZIONI DELLA FINALITÀ SCOPO 5

4.4. ESATTEZZA 5
4.5. LIMITAZIONE DELLA CONSERVAZIONE 5
4.6. INTEGRITÀ E RISERVATEZZA 5
4.7. RESPONSABILIZZAZIONE 5

5. FINALITÀ LEGITTIME PER IL TRATTAMENTO DEI DATI PERSONALI DEI DIPENDENTI 6

6. REQUISITI PER IL TRATTAMENTO DEI DATI PERSONALI DEI DIPENDENTI 6

6.1. COMUNICAZIONE AI DIPENDENTI 6
6.2. SCELTA E CONSENSO DEI DIPENDENTI 6
6.3. RACCOLTA 7
6.4. USO, CONSERVAZIONE E SMALTIMENTO 7
6.5. DIVULGAZIONE A TERZI 7
6.6. TRASFERIMENTO TRANSFRONTALIERO DEI DATI PERSONALI DEI DIPENDENTI 8
6.7. ACCESSO DEI DIPENDENTI 8

7. RESPONSABILITÀ 8

8. RISPOSTA IN CASO DI NON CONFORMITÀ 8

9. RESPONSABILIZZAZIONE 9

10. ECCEZIONI E VARIANTI 9

11. TITOLARE E CONTATTI 9

12. GESTIONE DELLE REGISTRAZIONI SULLA BASE DI QUESTO DOCUMENTO 9

13. VALIDITÀ E GESTIONE DEL DOCUMENTO 10

1. Campo d'applicazione, scopo e destinatari

La presente Politica disciplina la gestione dei Dati Personali relativi ai dipendenti di **PERITO GROUP S.R.L.** (da qui in avanti "L'Azienda") e fornisce regole e procedure applicabili a tutti i dipartimenti e a tutte le persone all'interno dell'Azienda, volte a garantire che i dati personali dei dipendenti siano trattati e protetti correttamente in tutti i paesi e le regioni.

Questa politica si applica al trattamento dei Dati Personali dei dipendenti da parte di qualsiasi dipartimento o individuo all'interno dell'Azienda, in tutti i paesi e le regioni.

" Azienda " si riferisce a **PERITO GROUP S.R.L.** e a tutte le società partecipate al 100% direttamente o indirettamente controllate dalla stessa ma esclude le società di joint venture.

Destinatari di questo documento sono tutti dipendenti dell'Azienda.

2. Documenti di riferimento

- Il GDPR dell'UE 2016/679 (Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio Europeo del 27 Aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE)
- D.Lgs. 30 giugno 2003, n. 196, come novellato dal Decreto Legislativo 10 agosto 2018, n.101 e dal decreto legislativo 18 maggio 2018, n. 51
- Politica sulla Protezione dei Dati Personali
- Politica di Conservazione dei Dati
- Politica sulla Violazione dei Dati
- Procedura sulla Violazione dei Dati

3. Definizioni

Le seguenti definizioni di termini utilizzati in questo documento sono tratte dall'articolo 4 del Regolamento Generale sulla Protezione dei Dati dell'Unione Europea (o GDPR):

3.1. Dato Personale

Qualsiasi informazione riguardante una persona fisica identificata o identificabile che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale. I Dati Personali includono l'indirizzo di posta elettronica di una persona fisica, il numero di telefono, le informazioni biometriche (come le impronte digitali), i dati di ubicazione, l'indirizzo IP, le informazioni sanitarie, le credenze religiose, il numero di previdenza sociale, lo stato civile eccetera.

3.2. Dati Personali Sensibili

Particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali, dal momento che la divulgazione di tali dati potrebbe portare a danni fisici, perdite finanziarie, danni alla reputazione, furto d'identità o frode o discriminazione ecc. I dati personali sensibili di solito comprendono, ma non sono limitati a, i dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati biometrici (impronte digitali) intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

3.3. Trattamento

Un'operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, la diffusione, la limitazione, la cancellazione o la distruzione dei dati.

3.4. Titolare del trattamento dei Dati:

La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del Trattamento di Dati.

4. Principi Generali per il Trattamento dei Dati Personali dei Dipendenti

4.1. Liceità, correttezza e trasparenza

I Dati Personali dei Dipendenti devono essere trattati in modo lecito, corretto e trasparente nei confronti del dipendente.

4.2. Limitazioni della finalità scopo

I Dati personali dei dipendenti devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità.

4.3. Minimizzazione dei dati

I Dati personali dei dipendenti devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati. Il **Responsabile delle Risorse Umane (o in mancanza il Responsabile amministrativo)** deve applicare l'anonimizzazione o la pseudonimizzazione ai Dati Personali dei dipendenti ove possibile per ridurre i rischi per i dipendenti interessati.

4.4. Esattezza

I Dati Personali dei Dipendenti devono essere esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati.

4.5. Limitazione della Conservazione

I Dati Personali dei Dipendenti devono essere conservati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati, in accordo alla Politica di Conservazione dei Dati.

4.6. Integrità e riservatezza

Tenuto conto dello stato della tecnologia e delle misure di sicurezza disponibili, dei costi di attuazione e della probabilità e gravità dei rischi per la privacy, i Dati Personali devono essere trattati in maniera da garantire un'adeguata sicurezza, compresa la protezione, mediante misure tecniche e organizzative adeguate dalla distruzione accidentale o illecita, perdita, modifica, accesso non autorizzato o divulgazione.

4.7. Responsabilizzazione

L'Azienda, in qualità di Controllore dei Dati personali dei dipendenti, sarà responsabile della conformità ai principi sopra descritti e dovrà essere in grado di dimostrarlo.

5. Finalità Legittime per il Trattamento dei Dati Personali dei Dipendenti

I dipartimenti o le persone all'interno dell'Azienda possono trattare i Dati personali dei dipendenti per finalità legittime che includono, a titolo esemplificativo ma non esaustivo:

Gestione delle risorse umane. Questo scopo comprende le attività di gestione delle risorse umane svolte durante l'assunzione o l'esecuzione di un contratto di lavoro, come colloqui, assunzione, cessazione del rapporto di lavoro, presenza, gestione delle prestazioni, indennità e benefici, formazione, servizi ai dipendenti, salute e sicurezza sul lavoro, e altre attività ai fini della gestione delle risorse umane o della protezione degli interessi vitali dei dipendenti.

Altre operazioni aziendali. Questo scopo comprende attività quali la gestione di viaggi e spese, la gestione di beni aziendali, la fornitura di servizi IT, la sicurezza delle informazioni, lo svolgimento di audit interni e indagini, l'adempimento degli obblighi di contratti commerciali, consulenza legale o aziendale e la preparazione a contenziosi legali, ecc.

Conformità con la legge. Il Trattamento dei Dati Personali dei Dipendenti al fine di adempiere a obblighi di legge, ad esempio: la divulgazione di Dati Personali dei dipendenti a un'autorità fiscale al fine di ottemperare alle leggi fiscali applicabili.

6. Requisiti per il Trattamento dei Dati Personali dei Dipendenti

Qualsiasi Trattamento dei Dati Personali dei dipendenti da parte di dipartimenti e individui all'interno dell'Azienda deve avvenire per uno scopo legittimo e deve soddisfare i seguenti requisiti:

6.1. Comunicazione ai Dipendenti

Ai fini della trasparenza del Trattamento dei Dati Personali dei dipendenti, quando un dipartimento o un individuo all'interno dell'Azienda raccoglie i dati personali di un dipendente, il dipendente deve essere informato dei tipi di dati raccolti, delle finalità e dei tipi di trattamento, dei diritti del dipendente e delle misure di sicurezza adottate per proteggere i Dati Personali. La comunicazione può assumere la forma della pubblicazione o dell'aggiornamento di dichiarazioni sulla protezione dei Dati Personali dei dipendenti, ad esempio: l'inserimento di termini sulla protezione dei Dati Personali dei dipendenti nei contratti di lavoro da parte del dipartimento Rapporti con I Dipendenti / Risorse Umane; l'inserimento della Dichiarazione dei Dati Personali nei sistemi IT pertinenti da parte del dipartimento Qualità, Processi Aziendali e gestione IT.

6.2. Scelta e Consenso dei Dipendenti

In linea di principio, l'Azienda può trattare i Dati Personali dei dipendenti per finalità legittime come datore di lavoro e generalmente può farlo senza ottenere il consenso del dipendente, per migliorare l'efficienza delle operazioni interne.

Le attività di gestione delle risorse umane come colloqui, assunzioni, cessazione del rapporto di lavoro, presenza, compensi e benefici, servizi dei dipendenti, salute e sicurezza sul lavoro possono comportare il Trattamento di Dati Personali Sensibili. Se leggi o regolamenti specifici di un Paese disciplinano tali questioni (ad esempio, ottenendo il consenso del dipendente), l'Azienda terrà conto di tali leggi o regolamenti.

6.3. Raccolta

I dipartimenti aziendali e le persone fisiche devono raccogliere i Dati Personali dei dipendenti per finalità legittime e devono rispettare il principio della Minimizzazione dei Dati. Se i Dati Personali di un candidato a un lavoro o di un dipendente sono raccolti da un terzo (ad esempio agenzie di collocamento o di controllo dei precedenti), l'Azienda deve fare il possibile per garantire questo terzo ottenga i Dati Personali con mezzi legittimi.

Nessun dipartimento aziendale o individuo può raccogliere i Dati Personali di candidati o dipendenti in modo non conforme alla legge o all'etica aziendale.

6.4. Uso, Conservazione e Smaltimento

I dipartimenti aziendali e gli individui devono utilizzare, conservare e disporre dei Dati Personali dei dipendenti in modo coerente con la comunicazione al dipendente. Devono inoltre garantire la sua esattezza, integrità e rilevanza. Devono essere messe in atto misure di sicurezza adeguate per proteggere i Dati Personali dei dipendenti da distruzione accidentale o illecita, perdita, modifica, accesso non autorizzato o divulgazione, in accordo alla politica di sicurezza delle informazioni e altri documenti che descrivono la sicurezza dei dati.

I dipartimenti aziendali e le persone fisiche non devono distruggere o modificare illecitamente i Dati Personali dei dipendenti. Non devono accedere, vendere o fornire illecitamente o senza autorizzazione Dati personali dei dipendenti a terzi.

Nel corso delle operazioni aziendali, il Responsabile della Protezione dei Dati deciderà se i Dati Personali dei dipendenti saranno trattati nei modi seguenti per ridurre al minimo il rischio per la protezione dei dati: i dati personali dei dipendenti possono essere anonimizzati ai fini della irreversibile deidentificazione; o i dati possono essere aggregati in risultati statistici o di ricerca. (I principi di Trattamento dei Dati Personali non si applicano ai dati resi anonimi e ai dati aggregati in quanto non sono Dati Personali.)

6.5. Divulgazione a Terzi

Quando i dipartimenti aziendali e gli individui devono comunicare i Dati Personali dei dipendenti a un fornitore, a un partner commerciale o a terzi, devono cercare di garantire che il fornitore, il partner

commerciale o altri terzi forniscano misure di sicurezza per salvaguardare i Dati Personali dei dipendenti che siano adeguate ai rischi associati. Dovrebbero inoltre richiedere al terzo di fornire lo stesso livello di protezione dei dati che forniscono all'Azienda per contratto o altro accordo.

Inoltre, quando i dipartimenti aziendali e gli individui rivelano i Dati Personali dei dipendenti in risposta a una richiesta da parte delle forze dell'ordine o di un'autorità giudiziaria, devono prima informare il Dipartimento Affari Legali che è autorizzato dall'Azienda a compiere uno sforzo coordinato per gestire la richiesta.

6.6. Trasferimento Transfrontaliero dei Dati Personali dei Dipendenti

Come organizzazione che opera a livello globale, l'Azienda trasferisce e tratta i Dati Personali dei dipendenti in tutto il mondo. Diversi paesi impongono requisiti diversi per il trasferimento transfrontaliero di Dati Personali (come ad esempio senza limitazioni, con limitazioni subordinate o il divieto di trasferire determinati tipi di Dati personali fuori dal paese). Prima di trasferire i Dati Personali da un paese, i dipartimenti aziendali e le persone fisiche devono consultare il Responsabile della Protezione dei Dati competente o l'ufficio Affari Legali per determinare se il trasferimento transfrontaliero sia necessario e legittimo.

Al momento del trasferimento dei Dati Personali dei dipendenti al di fuori dello Spazio Economico Europea, il cedente e il cessionario devono aver firmato un accordo di trasferimento dei dati in conformità con i regolamenti dell'UE e la Politica di Trasferimento Transfrontaliero dei Dati. Il cessionario deve fornire una protezione adeguata per i dati trasferiti in conformità con il contratto di trasferimento dei dati.

6.7. Accesso dei Dipendenti

I dipartimenti aziendali devono fornire mezzi ragionevoli ai dipendenti per accedere ai Dati Personali detenuti su di essi e consentire ai dipendenti di aggiornare, correggere, cancellare o trasmettere i propri Dati Personali se necessario o richiesto dalla legge. Quando si risponde a una richiesta di accesso di un dipendente, i dipartimenti aziendali possono non fornire alcun dato personale fino a quando non abbiano verificato l'identità del dipendente. L'azienda deve assicurarsi di conoscere l'identità della persona che effettua la richiesta prima di poter inviare i dati personali alla persona stessa.

7. Responsabilità

Il Reparto Risorse Umane (o in mancanza il Responsabile amministrativo) è competente per la gestione della protezione dei Dati personali dei dipendenti.

8. Risposta in Caso di Non Conformità

Chiunque sia a conoscenza di una violazione dei dati che coinvolga i Dati Personali dei dipendenti deve segnalarlo alle persone competenti all'interno dell'Azienda. Quando è necessario segnalare la violazione dei dati al di fuori della Società, si prega di seguire la Politica sulla Violazione dei Dati Personali.

Tuttavia, se richiesto dalla legge locale del paese in cui si è verificata la violazione dei dati, la persona designata nella Procedura di Risposta e Comunicazione di una Violazione dei Dati deve segnalare l'incidente al regolatore e / o alle parti interessate entro il periodo di riferimento specificato dalla legge.

9. Responsabilizzazione

Qualsiasi persona che violi questa Politica può essere soggetta ad azioni disciplinari interne (fino alla e compresa la cessazione del rapporto di lavoro) e può inoltre dover affrontare responsabilità civili o penali se la sua azione viola la legge.

10. Eccezioni e Varianti

I dipartimenti e le persone all'interno dell'Azienda dovrebbero anche fare riferimento a questa Politica quando trattano i Dati Personali di altro personale. "Altro personale" comprende: (1) le persone che cercano un impiego presso l'Azienda; (2) persone che sono state precedentemente assunte dall'Azienda; (3) altri non dipendenti dell'Azienda che lavorano presso strutture appartenenti all'Azienda (come dipendenti di partner che collaborano con l'Azienda, consulenti, stagisti).

11. Titolare e Contatti

Il Dipartimento Gestione Risorse Umane (o il Responsabile amministrativo) è titolare di questa politica ed è sua competenza interpretarla e gestirla.

12. Gestione delle registrazioni sulla base di questo documento

Nome del documento	Luogo di archiviazione	Persona responsabile dell'archiviazione	Controlli per la protezione del documento	Tempo di archiviazione
Contratti di Assunzione	Armadi con ante chiuse a chiave nel reparto	l'amministratore unico	Solo le persone autorizzate possono accedere a questi contratti.	10 anni dopo lo scioglimento

	Direzione Generale			del contratto di lavoro

13.Validità e gestione del documento

Questo documento ha effetto dal 18/01/2023.

Il responsabile per questo documento è il Responsabile amministrativo, il quale deve controllare e, se necessario, aggiornare il documento con frequenza almeno annuale.

Il Titolare

PERITO GROUP S.R.L.