1. CAMPO D'APPLICAZIONE, SCOPO E DESTINATARI

L'Azienda si impegna a rispettare le leggi e i regolamenti applicabili relativi alla protezione dei dati personali nei paesi in cui l'Azienda opera. Questa Politica stabilisce i principi di base con cui l'Azienda tratta i dati personali di consumatori, clienti, fornitori, partner commerciali, dipendenti e altre persone e indica le responsabilità dei propri dipartimenti aziendali e dipendenti durante il trattamento dei dati personali. La presente politica si applica all'Azienda e alle aziende che controlla direttamente o indirettamente che svolgono attività all'interno dello Spazio Economico Europeo (SEE) o che trattano i dati personali degli interessati all'interno del SEE. I destinatari di questo documento sono tutti i dipendenti, permanenti o temporanei, e tutti i collaboratori che lavorano per conto dell'Azienda.

2. DOCUMENTI DI RIFERIMENTO

- Il Regolamento (UE) 2016/679 del 27 Aprile 2016 (di seguito GDPR)
- Decreto legislativo n. 196 del 30 Giugno 2003 (Codice Privacy) e s.m.i.
- Politica di conservazione dei Dati
- Linee guida per l'elenco dei dati e la mappatura delle attività di trattamento
- Descrizione dei Ruolo del Responsabile della Protezione dei Dati
- Procedura per la richiesta di accesso ai dati da parte dell'interessato
- Metodologia di valutazione d'impatto sulla protezione dei dati
- Procedura di comunicazione di una violazione di dati
- Manuale SGI

3. OGGETTO E FINALITÀ

Il GDPR stabilisce le norme per la protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché le norme per la libera circolazione di tali dati (articolo 1).

4. AMBITO DI APPLICAZIONE MATERIALE

Nell'ambito di applicazione materiale del Regolamento vi sono:

- I dati personali sottoposti a trattamento interamente o parzialmente automatizzato.
- I dati personali contenuti in un archivio o destinati a esservi inseriti.

Fuori dall'ambito di applicazione materiale vi sono:

- I dati personali utilizzati nel corso di attività che non rientrano nell'ambito di applicazione del diritto dell'UE.
- I dati personali utilizzati nei controlli doganali e per le pratiche di asilo e immigrazione.
- I dati personali utilizzati in relazione ad attività puramente personali.
- I dati personali utilizzati a fini di prevenzione dei crimini, ecc.

5. AMBITO DI APPLICAZIONE TERRITORIALE

Il Regolamento si applica:

- I dati personali utilizzati nel corso di attività che non rientrano nell'ambito di applicazione del diritto dell'UE.
- I dati personali utilizzati nei controlli doganali e per le pratiche di asilo e immigrazione.

- I dati personali utilizzati in relazione ad attività puramente personali.
- I dati personali utilizzati a fini di prevenzione dei crimini, ecc.

6. DEFINIZIONI

Rispetto al Codice della Privacy (Decreto legislativo n. 196 del 30/06/2003) è stata eliminata la definizione di dati sensibili e di dati giudiziari; ora si parla di:

- Ai titolari e ai responsabili del trattamento nell'Unione, a prescindere dal luogo in cui avviene il trattamento.
- Ai titolari e ai responsabili del trattamento che non sono residenti nell'Unione quando le attività di trattamento riguardano:
- - Beni o servizi, a prescindere dal fatto che sia richiesto o meno un pagamento. - Il monitoraggio del comportamento degli interessati all'interno dell'UE.
- Ai titolari del trattamento non stabiliti nell'Unione, ma in un luogo in cui si applica il diritto di uno Stato membro.
- Categorie particolari di dati personali: dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
- Dati relativi alla salute: dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.
- Categorie particolari di dati personali: dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
- Dati genetici: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
- Dati biometrici: dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.
- Le seguenti definizioni di termini utilizzati in questo documento sono tratte dal Regolamento Generale sulla Protezione dei Dati dell'Unione Europea (GDPR):
- Dato Personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile («Interessato»); si considera identificabile la persona fisica 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.
- Titolare del trattamento dei dati (Titolare): 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 personali.
- Responsabile del trattamento dei dati (Data Processor DP): la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare.
- Responsabile della protezione dei dati (Data Protection Officer DPO): la persona fisica, la società, l'ente pubblico o privato, l'associazione o l'organismo cui il titolare affida, anche all'esterno della sua struttura organizzativa, specifici e definiti compiti di gestione e controllo del trattamento dei dati. La designazione di un DPO è obbligatoria:
  - se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico;
  - se le attività principali del titolare o del responsabile consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala; oppure - se le attività principali del titolare o del responsabile consistono nel trattamento su larga scala di categorie particolari di dati o di dati personali relativi a condanne penali e reati.
  La designazione obbligatoria di un DPO può essere prevista anche in casi ulteriori in base alla legge nazionale

o al diritto dell'Ue. Qualora si proceda alla designazione di un DPO su base volontaria, si applicano gli identici requisiti - in termini di criteri per la designazione, posizione e compiti - che valgono per i DPO designati in via obbligatoria (art. 37 GDPR).

- Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, 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, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

- Consenso dell'interessato: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.
- Violazione dei dati personali: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.
- Anonimizzazione : Deidentificazione irreversibile dei dati personali in modo tale che la persona non possa essere identificata utilizzando tempi, costi e tecnologie ragionevoli da parte del Titolare o di qualsiasi altra persona per identificare l'interessato. I principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile.
- Pseudonimizzazione: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile. La pseudonimizzazione riduce, ma non elimina completamente, la possibilità di collegare il dato personale all'interessato. Poiché i dati pseudonimizzati sono comunque dati personali, il trattamento dei dati pseudonimizzati dovrebbe essere conforme ai principi del trattamento dei dati personali.
- Trattamento transfrontaliero: trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un Titolare o DP dei dati nell'Unione ove il Titolare o il DP siano stabiliti in più di uno Stato membro; oppure il trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un Titolare o DP nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;
- Autorità di Controllo: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del GDPR dell'UE; per l'Italia è il Garante per la protezione dei dati personali (GARANTE) con sede in Piazza di Monte Citorio n. 121 - 00186 Roma - www.gpdp.it - www.garanteprivacy.it E-mail: garante@gsdp.it Fax: (+39) 06.69677.3785 Centralino telefonico: (+39) 06.69677.1

7. PRINCIPI APPLICABILI AL TRATTAMENTO DEI DATI PERSONALI

I principi applicabili alla protezione dei dati delineano le responsabilità delle organizzazioni nella gestione dei dati personali. Il Titolare è competente per il rispetto dei principi, e deve essere in grado di comprovarlo.

LICEITÀ, CORRETTEZZA E TRASPARENZA

I dati personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato. Il trattamento è lecito solo se e nella misura in cui ricorre almeno UNA delle seguenti condizioni:

- L'interessato ha espresso il consenso per una o più specifiche finalità.
- Il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte.
- Il trattamento è necessario per adempiere un obbligo legale del titolare del trattamento.
- Il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato.
- Il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio dei poteri di cui è investito il titolare del trattamento.

- Il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento.

LIMITAZIONE DELLE FINALITÀ

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

MINIMIZZAZIONE DEI DATI

I dati personali devono essere adeguati, pertinenti e limitati a quanto necessario in relazione alle finalità per cui sono trattati. L'azienda deve applicare l'anonimizzazione o la pseudonimizzazione ai dati personali, se possibile, per ridurre il rischio per gli interessati.

ESATTEZZA

I dati personali 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.

LIMITAZIONE DEL PERIODO DI CONSERVAZIONE

I dati devono essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati.

INTEGRITÀ E RISERVATEZZA

Tenendo conto delle tecnologie e di altre misure di sicurezza disponibili, dei costi di attuazione e la probabilità e gravità dei rischi per i dati personali, l'Azienda ha messo in atto misure tecniche e organizzative per garantire un livello di sicurezza adeguato per i dati personali, inclusa la protezione dalla distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati.

RESPONSABILIZZAZIONE

Il Titolare del trattamento dei dati è competente per il rispetto dei principi sopra descritti e attraverso la corretta applicazione ed osservazione della presente politica è in grado di comprovarlo.

8. PRINCIPI DI PROTEZIONE DEI DATI NELLE ATTIVITÀ COMMERCIALI

L'Azienda ha implementato i principi della protezione dei dati nel proprio sistema gestionale privacy, garantendo la conformità normativa delle diverse fasi operative, dalla raccolta al trattamento.

NOTIFICA AGLI INTERESSATI

(Vedi il capitolo Linee guida sul corretto trattamento.)

SCELTA E CONSENSO DELL'INTERESSATO

(Vedi il capitolo Linee guida sul corretto trattamento.)

RACCOLTA

Obiettivo dell'Azienda è adottare e migliorare costantemente i propri processi organizzativi ed operativi per raccogliere il minor numero di dati personali possibile. Se i dati personali sono raccolti da terzi, il responsabile del trattamento deve garantire che i dati personali siano raccolti legalmente. Manuale del Modello Organizzativo Privacy ai sensi del Regolamento (UE) 2016/679 Rev. 01 del 14/09/2018 DOCUMENTO AD USO INTERNO Pag. 13 di 44

USO, CONSERVAZIONE E SMALTIMENTO

Le finalità, i metodi, il limite di registrazione e il periodo di conservazione dei dati personali devono essere coerenti con le informazioni contenute nell'Informativa sulla Privacy. L'azienda deve mantenere l'esattezza, l'integrità, la riservatezza e la rilevanza dei dati personali in base allo scopo del trattamento. È necessario utilizzare adeguati meccanismi di sicurezza volti a proteggere i dati personali per impedire che vengano rubati, utilizzati in modo improprio o abusati e prevenire le violazioni dei dati personali. Il Titolare è responsabile della conformità con i requisiti elencati in questa sezione.

DIVULGAZIONE A TERZI

Ogni volta che la Società utilizza un fornitore o un partner commerciale terzo per il trattamento dei dati personali per suo conto, è necessario ottenere garanzie che questo fornisca misure di sicurezza per salvaguardare i dati personali adeguate ai rischi associati (per esempio uso inappropriato dei dati personali, divulgazione non autorizzata ecc). L'Azienda si impegna a richiedere contrattualmente al fornitore o partner commerciale di fornire un adeguato livello di protezione dei dati (Modulo GDPR-NRET Nomina Responsabile Esterno Trattamento). I fornitori o i partner commerciali devono trattare i dati personali solo per adempiere ai propri obblighi contrattuali nei confronti dell'Azienda o dietro istruzioni dell'Azienda e non per altri scopi. Quando l'Azienda tratta i dati personali congiuntamente con un terzo indipendente, essa deve specificare esplicitamente le responsabilità proprie e quelle del terzo nel relativo contratto o qualsiasi in altro documento legalmente vincolante.

TRASFERIMENTO TRANSFRONTALIERO DEI DATI PERSONALI

L'Azienda non esegue trasferimenti di dati personali all'estero, comunque eventualmente prima di trasferire i dati personali dallo Spazio Economico Europeo (SEE) devono essere utilizzate misure di protezione adeguate, compresa la firma di un accordo sul trasferimento dei dati, come richiesto dall'Unione Europea e, se necessario, deve essere ottenuta l'autorizzazione della relativa Autorità per la Protezione dei Dati.

DIRITTO D'ACCESSO DA PARTE DEGLI INTERESSATI

L'azienda è responsabile di fornire agli interessati un ragionevole meccanismo di accesso per consentire loro di accedere ai propri dati personali e deve consentire loro di aggiornare, rettificare, cancellare o trasmettere i propri dati personali, se del caso o richiesto dalla legge. Il meccanismo di accesso sarà ulteriormente dettagliato nella Procedura di richiesta di accesso ai dati da parte dell'Interessato.

PORTABILITÀ DEI DATI

Gli interessati hanno il diritto di ricevere, su richiesta, una copia dei dati che ci hanno fornito in un formato strutturato e di trasmettere tali dati a un altro Titolare, gratuitamente. L'azienda è responsabile di garantire che tali richieste vengano elaborate entro un mese, non siano eccessive e non incidano sui diritti relativi ai dati personali di altre persone.

DIRITTO ALL'OBLIO

Su richiesta, gli interessati hanno il diritto di ottenere dall'Azienda la cancellazione dei propri dati personali se sussiste uno dei seguenti motivi:

- I dati personali non sono più necessari rispetto alle finalità per le quali erano stati raccolti o altrimenti trattati.
- L'interessato revoca il consenso su cui si basa il trattamento e non sussiste altro fondamento giuridico per il trattamento.
- L'interessato si oppone al trattamento e non sussiste alcun motivo legittimo prevalente per procedere al trattamento.
- I dati personali sono stati trattati illecitamente.
- I dati personali devono essere cancellati per adempiere un obbligo legale.

9. LINEE GUIDA SUL CORRETTO TRATTAMENTO

I dati personali devono essere trattati solo se esplicitamente autorizzati dal Titolare del trattamento. Il Titolare stabilisce se eseguire la Valutazione d'Impatto sulla protezione dei dati per ciascuna attività di trattamento dei dati in base alle Linee guida sulla Valutazione d'Impatto sulla protezione dei dati.

COMUNICAZIONI AGLI INTERESSATI

Al momento della raccolta o prima della raccolta di dati personali per qualsiasi tipo di attività di trattamento, ma non limitata alla vendita di prodotti, servizi o attività di marketing, il Titolare è responsabile di informare adeguatamente gli interessati di quanto segue:

- l'identità e i dati di contatto del Titolare del trattamento;
- se nominato, l'identità e i dati di contatto del Responsabile della Protezione dei dati (DPO);
- modalità e finalità del trattamento dei dati;
- presupposti giuridici al trattamento dei dati;
- categorie di destinatari;
- i potenziali trasferimenti dei dati (eventuale);
- il periodo di conservazione;
- i diritti dell'interessato riguardo ai suoi dati personali;
- se i dati saranno condivisi con terzi e le misure di sicurezza stabilite dall'Azienda per proteggere i dati personali;
- le conseguenze del mancato consenso al trattamento.

Queste informazioni sono fornite tramite l'Informativa sulla Privacy (Modello GDPR-IC per i Clienti; GDPR-IF per i Fornitori). L'azienda inoltre, in osservanza del principio di Accountability (responsabilizzazione) dovrà ottenere dall'interessato la conferma che lo stesso ha letto e compreso il contenuto dell'informativa mediante apposita dichiarazione sulla copia della stessa.

OTTENERE I CONSENSI

Ogni volta che il trattamento dei dati personali si basa sul consenso dell'interessato, o su altri motivi legittimi, il Titolare è responsabile:

- della conservazione di una registrazione di tale consenso (mediante conservazione del modulo di informativa sottoscritto dall'interessato);
- di fornire agli interessati le opzioni per dare il consenso;
- di informare gli interessati e garantire loro come il consenso prestato (ogni volta che il consenso venga utilizzato come base legale per il trattamento) possa essere revocato in qualsiasi momento.

Laddove la raccolta di dati personali si riferisca a un minore di età inferiore ai 16 anni, il Titolare deve garantire che il consenso del titolare della responsabilità genitoriale sia fornito prima della raccolta utilizzando il modulo specifico. Quando si richiede di correggere, modificare o distruggere le registrazioni dei dati personali, il Titolare deve garantire che tali richieste siano gestite entro un ragionevole lasso di tempo e deve anche registrare le richieste e tenere un registro di queste. I dati personali devono essere trattati solo per le finalità per cui sono stati originariamente raccolti. Nel caso in cui l'Azienda desideri trattare i dati personali raccolti per un altro scopo, l'Azienda deve richiedere il consenso degli interessati in forma scritta chiara e concisa. Qualsiasi richiesta di questo tipo dovrebbe includere lo scopo originale per cui sono stati raccolti i dati e anche gli scopi nuovi o aggiuntivi. La richiesta deve includere anche il motivo del cambiamento di scopo. Ora e in futuro, il Titolare deve garantire che i metodi di raccolta siano conformi alla legge, alle buone pratiche e alle norme industriali pertinenti. Il Titolare è responsabile della creazione e della manutenzione di un registro delle Informative sulla Privacy.

TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI PERSONALI

È vietato trattare dati personali che rivelino:

- razza;
- origine etnica;
- opinioni politiche;
- convinzioni religiose;
- convinzioni filosofiche;
- appartenenza sindacale;
- dati genetici;
- dati biometrici;
- dati relativi alla salute;
- vita sessuale di una persona;
- orientamento sessuale.

Eccezioni: l'interessato ha prestato il proprio consenso esplicito;

- Il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;
- il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
- il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;
- i dati personali sono resi manifestamente pubblici dall'interessato;
- il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
- il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;
- il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità;
- il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale;
- il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici

La liceità del trattamento è un prerequisito.

10. 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.

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. Queste informazioni sono fornite da apposita Informativa al trattamento dei dati personali (Modulo GDPR-ID).

COMUNICAZIONE AI CANDIDATI

La stessa trasparenza garantita per il trattamento dei dati personali dei dipendenti è assicurata anche per la raccolta dei dati personali di un candidato in fase di colloquio per una possibile assunzione. Il candidato deve essere informato dei tipi di dati raccolti, delle finalità e dei tipi di trattamento, dei suoi diritti e delle misure di sicurezza adottate per proteggere i dati personali. Queste informazioni sono fornite da apposita Informativa al trattamento dei dati personali (modello GDPR-ICL).

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 sicurezza e 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.

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 lavoro interinale), l'Azienda deve fare il possibile per garantire che 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.

USO, CONSERVAZIONE E SMALTIMENTO

I dipartimenti aziendali e le persone fisiche 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. L'azienda ha messo in atto misure di sicurezza adeguate a 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 Titolare 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).

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 (Modulo GDPR-NRET). 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 Responsabile della protezione dei dati (DPO) che è autorizzato dall'Azienda a compiere uno sforzo coordinato per gestire la richiesta.

TRASFERIMENTO TRANSFRONTALIERO DEI DATI PERSONALI DEI DIPENDENTI

L'azienda non effettua trasferimenti transfrontalieri dei dati, comunque nel caso in cui si rendesse necessario farlo, prima di trasferire i dati personali, i dipartimenti aziendali e le persone fisiche devono consultare il Responsabile della Protezione dei dati (DPO) o il Titolare del trattamento per determinare se il trasferimento transfrontaliero sia necessario e legittimo.

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.

RESPONSABILITÀ

Il Reparto Risorse Umane è competente per la gestione della protezione dei dati personali dei dipendenti.

11. ORGANIZZAZIONE AZIENDALE

Il GDPR introduce nuovi obblighi organizzativi. La responsabilità di garantire un adeguato trattamento dei dati personali spetta a chiunque lavori per o con l'Azienda e abbia accesso ai dati personali trattati dall'Azienda; a tal fine l'Azienda ha implementato un proprio organigramma Privacy.

Le principali aree di responsabilità sono identificabili nei seguenti ruoli organizzativi: Il Titolare del trattamento dei dati, prende decisioni e approva le strategie generali della Società in materia di protezione dei dati personali. Tale ruolo è ricoperto dal legale rappresentante pro-tempore. Il Responsabile della Protezione dei Dati (RPD/DPO), è responsabile della gestione del programma di protezione dei dati personali ed è responsabile dello sviluppo e della promozione delle politiche di protezione dei dati personali dall'inizio alla fine, come definito nella Descrizione del Ruolo del Responsabile della Protezione dei Dati. L'Amministratore di sistema, è responsabile di:

- garantire che tutti i sistemi, i servizi e le attrezzature utilizzati per la registrazione dei dati soddisfino standard di sicurezza accettabili.
- Condurre controlli e scansioni regolari per garantire che l'hardware e il software di sicurezza funzionino correttamente.

L'Internal Audit, è responsabile delle verifiche interne volte al rispetto delle procedure e delle politiche sulla protezione dei dati personali. Le Persone autorizzate, dipendenti formalmente autorizzati a compiere operazioni di trattamento dal titolare.

12. OBBLIGHI GENERALI

REGISTRI DELLE ATTIVITÀ DI TRATTAMENTO

Il Titolare del trattamento deve tenere un registro delle attività di trattamento contenente le seguenti informazioni:

- dati di contatto del Titolare del trattamento e, dove applicabile, del contitolare del trattamento e del Responsabile della protezione dei dati;
- finalità del trattamento;
- categorie di interessati;
- categorie di dati personali trattati;
- categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

RISPOSTA AGLI INCIDENTI DI VIOLAZIONE DEI DATI PERSONALI

Quando l'Azienda viene a conoscenza di una presunta o effettiva violazione dei dati personali, il Titolare coadiuvato dal DPO deve eseguire un'indagine interna e adottare misure correttive appropriate in modo tempestivo, in base alla Procedura di risposta e comunicazione della violazione dei dati.

AUDIT E RESPONSABILIZZAZIONE

L'Internal Audit è responsabile di verificare in che modo i reparti aziendali implementino questa politica. Qualsiasi dipendente che violi questa Politica sarà soggetto ad azioni disciplinari e potrebbe anche essere soggetto a responsabilità civili o penali qualora la sua condotta violasse leggi o regolamenti.

CONFLITTI CON LA LEGGE

Questa politica è intesa a rispettare le leggi e i regolamenti del luogo di stabilimento e dei paesi in cui opera l'Azienda