Titolo Politica:	**Politica sulla protezione dei dati**
Titolare Politica:	**Responsabile Affari Legali e VP Senior del dipartimento Risorse Umane**
Dipartimento:	**Risorse Legali e Umane**
Data di entrata in vigore:	**24 maggio 2018**
Data di revisione:	
Data nuova revisione:	**24 maggio 2019**

POLITICA SULLA PROTEZIONE DEI DATI: REGOLE GENERALI

I dipendenti di NEP Group ("Nep" o "l'Azienda") sono responsabili per quanto riguarda la protezione di informazioni relative all'azienda e ai dipendenti NEP, indipendentemente dal mezzo.

Per ulteriori dettagli e informazioni, si prega di leggere il testo della presente politica.

INDICE:

NOTA INTEGRATIVA E STATUS DELLA PRESENTE POLITICA

Nella presente politica NEP Group, Inc. e le sue filiali vengono indicate come "**NEP**", la/le "**Azienda/e**", "**noi**", "**ci**", "**nostro**". NEP ha bisogno di raccogliere ed elaborare un certo numero di informazioni relative ai singoli individui per poter gestire efficacemente i suoi affari. Le informazioni provengono, fra le altre cose, da dipendenti attuali, passati e potenziali, da lavoratori, candidati, clienti, accreditatori, fornitori e altri individui con i quali NEP comunica o ha rapporti di lavoro.

Siamo responsabili della nostra responsabilità nel trattamento delle informazioni di questi individui, informazioni che verranno gestite con attenzione e nel rispetto delle leggi sulla privacy e sulla protezione dei dati ("**Leggi sulla Protezione dei Dati**"). Il nostro brand e i nostri valori organizzativi ci richiedono di adottare e di rispettare le procedure di governance per una corretta gestione dei dati, incluse quelle previste nella Politica di Protezione dei Dati ("**Politica**").

Nella Sezione A della presente Politica viene stabilito come NEP utilizzerà i dati relativi al suo personale, mentre nella Sezione B, vengono stabilite delle linee guida su determinate misure fondamentali che NEP si aspetta vengano rispettate dal suo personale quando si tratta di attività legate al trattamento dei dati NEP. La presente politica stabilisce le nostre norme in merito alla protezione dei dati e le condizioni che devono essere rispettate riguardo a l'ottenimento, la gestione, il trattamento, la registrazione, il trasporto e la distruzione di informazioni personali.

Nel rispetto delle leggi vigenti, la presente Politica si applica a tutti i dipendenti NEP (che lavorano a tempo pieno o a mezza giornata), ai dipendenti temporanei, ai fornitori di servizi esterni, ai volontari, agli stagisti, ai visitatori, ai venditori e a terzi.

Per le zone NEP in cui la legge in vigore richieda politiche specifiche e/o procedure che sostituiscano o che debbano essere aggiunte alla presente Politica, degli addendum specifici al paese possono essere allegati alla presente Politica.

SEZIONE A – LE RESPONSABILITÀ CHE NEP HA NEI VOSTRI CONFRONTI SECONDO LA LEGGE SULLA PROTEZIONE DEI DATI

1. Team responsabile per la Privacy dei Dati

NEP ha nominato un team di Responsabili per la Protezione dei Dati che aiuta l'Azienda a rispettare le obbligazioni previste dalle Leggi sulla Protezione dei Dati. Il ruolo fondamentale che viene svolto dai Responsabili per la Protezione dei Dati è il seguente:

- fornire un punto di contatto e di supporto per il personale;
- svolgere e partecipare alla realizzazione di valutazioni d'impatto sulla privacy;
- fornire formazione per il personale;
- cooperare con l'autorità locale che si occupa della protezione dei dati;
- gestire le richieste d'accesso alle informazioni; e

se in seguito alla lettura della presenta Politica o in qualsiasi momento ci dovessero essere delle domande relative a come si dovrebbero gestire i Dati Personali, si prega di contattare il Responsabile per la Protezione dei Dati locale.

Il contatto del Responsabile per la Protezione dei Dati locale può essere recuperato contattando l'ufficio Legale, le Risorse Umane o l'Ufficio IT.

2. Ambito di applicazione delle leggi per la protezione dei dati

Le Leggi sulla Protezione dei Dati stabiliscono il modo in cui NEP deve gestire le informazioni che identifica o le informazioni che riguardano persone viventi (Dati Personali). Conferiscono inoltre determinati diritti e mezzi di ricorso a cui gli individui possono fare appello a riguardo di tali informazioni. Le leggi regolano inoltre le attività di marketing e l'utilizzo di tecnologie di monitoraggio online, come i cookies. Queste includono un'ampia area di attività che NEP (nonché i partner e i fornitori che lavorano per conto di NEP) svolge.

Le leggi impongono uno standard più elevato in merito all'utilizzo di "**Dati Personali Sensibili**" che includono informazioni riguardanti le origini razziali o etniche di un individuo, le opinioni politiche, le credenze religiose e le convinzioni filosofiche; l'appartenenza a un sindacato, lo stato di salute, la vita sessuale, l'orientamento sessuale, i dati biometrici e genetici, e per lo scopo della presente politica, le condanne e i reati penali. Nella presenta politica, quando si parla di "**Dati Personali**" si vuole fare riferimento a tutte quelle attività che vengono svolte utilizzando qualsiasi tipo di Dati Personali Sensibili.

Le Leggi sulla Protezione dei Dati regolano le informazioni conservate in versione digitale da o a nome di NEP, o in alcune situazioni, conservate in sistemi ben organizzati, di archiviazione manuale. Sono incluse le videoregistrazioni con telecamere a circuito chiuso e le registrazioni vocali.

3. Generi di informazione che NEP può avere in suo possesso in merito al suo personale

I generi di Dati Personali che NEP potrà utilizzare durante il rapporto con l'utente prevedono:

- nomi, indirizzi, numeri di telefono e altri dettagli di contatto personali;
- genere, data di nascita, numero di assicurazione nazionale/numero di carta d'identità, stato di immigrazione, stato civile, parenti più stretti;
- informazioni relative al personale che riguardano formazione, valutazioni, fotografie, performance e informazioni disciplinari, informazioni in merito a disabilità, curriculum e pianificazione di promozione;
- coordinate bancarie, dettagli sullo stipendio, bonus, benefit e pensione;
- immagini TVCC e registrazioni di chiamate;
- i viaggi effettuati, copie di passaporti, copie delle patenti di guida, password, identificanti e informazioni relative all'idoneità di ottenere un visto.

- Dati Personali Sensibili come informazioni relative all'origine razziale o etnica, credenze religiose e convinzioni filosofiche; appartenenza a un sindacato, stato di salute, vita sessuale, orientamento sessuale, dati biometrici e genetici, condanne e reati penali.

4. Come NEP può trattare i Dati Personali

I Dati Personali relativi a individui possono essere trattati solo per scopi legittimi. NEP intraprenderà una serie di attività con i Dati Personali di un membro del personale per, ma non solo:

- amministrare lo stipendio, i benefit e le indennità;
- gestire e registrare dati relativi allo stato di salute e della sicurezza;
- effettuare controlli sulla fedina penale, sul credito e su eventuali autorizzazioni (se il caso sussiste);
- confermare le informazioni che appaiono sul curriculum, lettere di motivazione, lettere di referenza e per effettuare controlli sulle stesse;
- formare e valutare, compresa la valutazione delle performance e dei precedenti disciplinari;
- gestire il personale e le eventuali promozioni;
- i piani di successione;
- verificare le pari opportunità;
- qualsiasi genere di cambio di gestione di un'azienda del gruppo, o qualsiasi potenziale trasferimento di ruolo, che possa essere collegato a un trasferimento dell'impresa o del fornitore (in Europa, secondo la Direttiva sui Diritti Acquisiti). In questo genere di circostanze, i Dati Personali possono esclusivamente essere divulgati a potenziali acquirenti o investitori e ai loro consulenti nella misura consentita dalla legge applicabile;
- altre divulgazioni richieste durante la fase di assunzione del personale che servono a promuovere o a pubblicizzare NEP, i suoi prodotti o servizi;
- divulgazione di informazioni relative al personale, a clienti e agenzie nell'ambito dello svolgimento dei loro servizi presso NEP;
- monitoraggio TVCC per motivi di sicurezza;
- gestione di qualsiasi genere di hotline che riguardi l'etica o la denuncia di irregolarità che NEP può gestire ora o in futuro;
- rispetto delle procedure applicabili, leggi, regolamenti, incluse tutte quelle indagini che garantiscono il rispetto delle procedure o possibili violazioni;
- stabilire, esercitare o difendere i diritti legali di NEP;
- qualsiasi altro scopo ragionevole che sia direttamente connesso con l'assunzione di un individuo o del suo impegno con NEP;
- fornire e gestire l'utilizzo di servizi proposti da terzi, quali agenzie di viaggio, telefoni aziendali, carte di credito aziendali e macchine aziendali e la fatturazione di tali servizi.

NEP può inoltre raccogliere e trattare i Dati Personali dei parenti più stretti affinché possano essere contatti in caso di emergenza o per quanto riguarda l'utilizzo della macchina aziendale fornita da NEP. I loro Dati Personali saranno inoltre trattati secondo le Leggi per la gestione dei Dati Personali e come descritto nella presente Politica.

Per conseguire tali obiettivi, NEP si riserva il diritto di divulgare a sua discrezione i Dati Personali di un individuo (o informazioni personali sensibili ove opportuno) alle forze dell'ordine, alle autorità normative, agli enti governativi e a terzi come richiesto dalla legge o per scopi amministrativi, nella misura in cui la legge locale lo permetta e lo richieda.

NEP può inoltre fornire i Dati Personali per gli scopi sopra citati, ma non solo, può fornirli agli appaltatori e a coloro che forniscono dei servizi a NEP e che possono assisterla nelle attività di trattamento sopra citate. In tal caso, NEP si impegna inoltre di stipulare un contratto sul trattamento dei dati, con gli appaltatori e i fornitori che ricevono i Dati Personali da parte di NEP.

NEP può trasferire i Dati Personali ad altre società del gruppo, a partner, fornitori, alle forze dell'ordine e ad altre organizzazioni situate al di fuori dello Spazio economico europeo ("**SEE**") (a tale scopo anche il Regno Unito viene incluso) per i seguenti motivi:

- amministrazione delle Risorse Umane (per esempio, assunzione del personale);
- elaborazione delle buste paghe del personale che lavora al di fuori del SEE;
- trasferimento del personale;
- domande di visto;
- tassazione e registrazioni per il personale che lavora al di fuori del SEE;
- soddisfare i requisiti legali di NEP;
- soddisfare i contratti concordati con i clienti per la fornitura dei servizi a NEP;
- procedimenti legali d'oltremare; e
- delocalizzare le attività di NEP.
- Certificazioni e visti di viaggio.

Questi paesi possono includere, tra gli altri, i paesi nei quali NEP svolge le sue operazioni e il luogo dove sono situati i nostri fornitori e i loro centri di gestione dei dati, come Microsoft (Stati Uniti), oltre ad altri importanti fornitori di programmi di gestione per le Risorse Umane.

Si prega di notare che le leggi di alcune giurisdizioni situate al di fuori del SEE potrebbero non essere così protettive riguardo alle leggi sul trattamento dei Dati Personali del SEE.

5. Conservazione dei dati

Per legge, NEP ha il dovere di conservare alcuni dati per un periodo di tempo minimo. NEP non deve conservare i Dati Personali per un periodo superiore rispetto al periodo necessario o a quanto richiesto dalla legge in vigore.

6. Verifica

Sistemi di verifica NEP

I sistemi di comunicazione e i sistemi informatici di NEP hanno lo scopo di promuovere una comunicazione efficace e pratiche di lavoro all'interno della nostra organizzazione.

Per motivi aziendali, e per rispettare le misure di sicurezza dei sistemi informatici, l'utilizzo di sistemi NEP su piattaforme specifiche, inclusi i sistemi telefonici (cellulare e fisso) e informatici (accesso alle email e a internet), nonché l'eventuale uso personale, sono monitorati. Nel caso in cui l'utente utilizzasse delle password e dei nomi utente per connettersi ai sistemi informatici e di comunicazione NEP, ciò significa che i dettagli dell'accesso personale dell'utente sono monitorati da NEP.

Questa verifica viene effettuato solo se e nella misura prevista dalla legge e se necessario e giustificabile per scopi commerciali. Questo viene richiesto per poter individuare possibili abusi ed eventi che potrebbero rappresentare una minaccia alla sicurezza e per poter disporre di informazioni che potrebbero essere utilizzate come supporto di eventuali indagini e azioni successive. Nella misura consentita dalla legge e in caso di violazioni della presente Politica, delle azioni possono essere intraprese in base alla procedura disciplinare.

NEP si riserva il diritto di recuperare il contenuto di messaggi, verificare ricerche effettuate su internet, richiedere la restituzione immediata di dispositivi forniti da NEP e di accedere ai dati memorizzati su tali dispositivi per i motivi seguenti (questa lista non è esaustiva):

- verificare che la posta elettronica o internet siano stati utilizzati rispettando la presente Politica (il personale è a conoscenza che NEP possa utilizzare dei programmi per verificare l'identità degli emittenti e dei destinatari delle email);
- per cercare messaggi andati perduti o per recuperare messaggi persi a causa di un malfunzionamento del computer;
- per contribuire all'indagine di atti illeciti, inclusi tutti quegli atti che violano le nostre altre politiche o la legge in vigore; e
- per adempiere a qualsiasi obbligo legale.

Una condizione che deve essere rispetta per poter utilizzare i nostri sistemi informatici e che si tenga un comportamento professionale, che non si screditi il buon nome dell'azienda e che non si tenga un comportamento inappropriato nei confronti di colleghi o altre persone con le quali si potrebbe entrare in contatto durante il periodo lavorativo presso NEP. Qualora venissero rinvenute prove di una violazione di tali condizioni o di un uso improprio dei sistemi informatici di NEP, NEP, conformemente alle procedure disciplinari aziendali, ha il diritto di intraprendere un'indagine più dettagliata, che includa l'analisi e la divulgazione dei dati monitorati a coloro che sono stati incaricati di svolgere l'indagine e a qualsiasi testimone che sia coinvolto con la procedura disciplinare. La stessa cosa può avvenire se NEP ha motivi fondati di sospettare che attività o azioni illegali, che potrebbero violare le nostre altre politiche e procedure, sono avvenute.

Se necessario, queste informazioni possono essere passate nelle mani della polizia o di altre forze dell'ordine. Le indagini e la divulgazione di tali informazioni alle autorità competenti possono avvenire solo nella misura consentita dalla legge.

Videosorveglianza circuito chiuso

Alcuni edifici di NEP e alcune aree utilizzano sistemi di videosorveglianza a circuito chiuso per monitorare gli esterni e gli interni 24 ore su 24, per motivi di sicurezza. Questi dati vengono registrati. L'utilizzo di sistemi di videosorveglianza a circuito chiuso e la registrazione di dati tramite i sistemi di videosorveglianza a circuito chiuso vengono gestiti secondo le linee guida approvate da NEP.

7. Diritti dell'utente sui dati

Secondo la legge sulla Protezione dei Dati i membri del personale hanno il diritto di chiedere a NEP una copia dei loro Dati Personali, per correggerli, cancellarli o ridurne il trattamento, o di chiedere a NEP di trasferire alcune informazioni ad altre organizzazioni. Il personale ha inoltre il diritto di opporsi ad alcuni dei trattamenti dei Dati Personali e, nel caso in cui NEP avesse chiesto il consenso dei Dati Personali, il personale ha diritto di ritirarlo. Questi diritti, in alcune situazioni, possono essere limitati - per esempio, nel caso in cui NEP dimostri di avere l'obbligo legale di trattare i dati dell'utente. In alcuni casi, ciò significa che NEP può conservare i dati nonostante il membro del personale ne abbia ritirato il consenso.

La dove viene richiesto da NEP di fornire Dati Personali per rispettare gli obblighi legali o contrattuali, fornire tali dati è obbligatorio: se tali dati non vengono forniti, NEP non sarà in grado di gestire il rapporto di lavoro o di rispettare gli obblighi che ci sono stati richiesti. In tutti gli altri casi, il conferimento dei Dati Personali richiesti è facoltativo.

Per qualsiasi altra informazione o domande su come NEP tratti i Dati Personali dei suoi dipendenti, si prega di contattare il team responsabile per la Protezione dei Dati.

8. Reclami

Un lavoratore che ritenga che un'altra persona possa avere violato i suoi diritti sulla protezione dei dati è incoraggiato a segnalarlo al suo responsabile diretto o a qualsiasi altra persona così come viene specificato nella procedura relativa alla gestione locale dei reclami/nell'ambito dell'unità operativa.

I dipendenti con problemi irrisolti hanno anche il diritto di rivolgersi alle autorità competenti in materia di protezione dei dati. L'autorità competente in materia di protezione dei dati corrisponde all'autorità di controllo presente nello stesso paese del datore di lavoro.

Sezione A - Le responsabilità dell'utente nei confronti di terzi ai sensi delle Leggi sulla protezione dei dati

Questa parte della Politica ha come scopo quello di informare il personale riguardo a come dovrebbero essere gestiti i Dati Personali in alcune circostanze. Ogni membro del personale ha l'obbligo di rispettare le Leggi sulla Protezione dei Dati. È importante che gli individui siano a conoscenza delle loro responsabilità nei confronti di terzi, previste dalle Leggi sulla Protezione dei Dati, che richiedono di seguire le linee guida e i procedimenti previsti qui di seguito. Ecco alcuni punti chiave che devono essere ricordati dall'utente:

- prendere conoscenza delle loro responsabilità, previste dalle Leggi sulla Protezione dei Dati e dalla presente Politica e sull'impatto che tali responsabilità possono avere sulle loro attività quotidiane.
- Condividere i Dati Personali (o dati sensibili da un punto di vista commerciale) esclusivamente sulla base delle esigenze del momento. Non condividere un database intero se ne viene richiesta soltanto una parte.
- Verificare due volte se il destinatario è corretto, prima di condividere i dati. Chiedersi se i dati che stanno per essere trasmessi abbiano come scopo quello di ledere o di mettere a rischio l'azienda.
- Se necessario, utilizzare password per proteggere file dove richiesto.
- Utilizzare i Dati Personali solo nel modo in cui è stato concordato con la persona interessata o come è stato previsto dalla presente Politica.
- Adottare buon senso quando si decide su come proteggere, usare e disporre dei Dati Personali. L'utente deve riflettere a come vorrebbe che venissero trattate le sue informazioni personali.

Questa sezione ha come scopo quello di fornire delle linee guida generali e non vuole essere una guida completa o esaustiva. In base alla natura del lavoro, all'utente potrebbe essere richiesto di avere maggiori responsabilità rispetto ad altri in merito alle Leggi sulla Protezione dei Dati.

Le responsabilità generali dell'utente riguardano:

9. Principi sulla protezione dei dati

Nel trattamento dei Dati Personali, NEP e i membri del personale devono rispettare alcuni principi riguardanti il trattamento dei dati personali previsto dalle Leggi sulla protezione dei Dati Personali. Queste leggi prevedono che i Dati Personali:

- siano trattati in modo giusto e legale;
- siano trattati solo per uno o più scopi determinati e legittimi, e che non siano trattati successivamente in modo incompatibile con tali scopi a meno che non sia espressamente consentito dalle leggi in vigore;
- siano adeguati, pertinenti e che non siano fuori luogo rispetto al motivo per cui sono stati trattati;
- siano precisi, e là dove necessario, che vengano aggiornati;
- che non siano conservati per più tempo del dovuto al conseguimento delle finalità per le quali sono stati trattati;
- che siano trattati rispettando i diritti dell'individuo, e in alcune circostanze di avere il diritto: di accedere ai Dati Personali, di trasmetterli a terze parti, di essere cancellati, nel caso in cui fossero errati o non fossero più richiesti e di non essere soggetti a nessuna decisione automatizzata rilevante;
- siano conservati al sicuro; e
- che siano trasferiti a o accessibili da un paese o da un territorio al di fuori del SEE se il paese in questione garantisce un livello adeguato di protezione, in merito ai diritti e alle libertà degli

individui riguardo il trattamento dei Dati Personali, o in paesi in cui siano previste adeguate garanzie contrattuali per la protezione dei dati.

10. Mantenere i dati al sicuro

I provvedimenti di questa sezione e della sezione 11 (segnalazione di sospette violazioni della sicurezza dei dati) non solo si riferiscono ai Dati Personali ma a tutte quelle informazioni, sistemi informatici e di comunicazione, per cui l'utente è responsabile, per la sicurezza degli strumenti che gli sono stati conferiti o che vengono utilizzati dallo stesso, e che non devono essere usati da nessun altro se non nel rispetto della presente Politica.

Sicurezza del computer e del portatile:

- Tutti coloro che utilizzano i sistemi informatici riceveranno delle credenziali personali. Account o password non devono essere condivisi. L'utente non deve utilizzare gli account che non gli appartengono e non deve divulgare a terzi, le informazioni del suo account.
- In tutti quei momenti in cui il computer, il portatile o i dispositivi palmari dovessero rimanere incustoditi (per esempio durante incontri o pausa pranzo) devono essere bloccati con una password, la sessione deve essere disconnessa o dovranno essere spenti. Il sistema informatico di NEP è stato progettato in modo tale che, quando possibile, si blocchi o si spenga automaticamente dopo un certo periodo di inattività.
- Alla fine di ogni giornata lavorativa l'utente dovrà assicurarsi che il suo computer e monitor siano stati spenti dovutamente. Nel caso in cui si possedesse un portatile, deve essere conservato in modo sicuro, per esempio in uno stipetto o in un cassetto chiuso a chiave.
- Assicurarsi che le informazioni confidenziali e sensibili dell'azienda riproducibili sullo schermo non siano visibili al di fuori dell'azienda.
- Utilizzare una password sicura (per esempio un insieme di lettere maiuscole e minuscole, numeri e caratteri speciali) e non divulgarla a nessuno. Cambiarla regolarmente e nel caso in cui l'utente ritenesse che altri la conoscono, si prega di cambiarla immediatamente.
- Le modifiche o la manutenzione che avvengono sul computer o sui dispositivi informatici dell'utente, di tipo hardware o software su risorse supportate da NEP, devono essere eseguiti esclusivamente dal team dei Servizi informatici NEP, da partner associati o da individui autorizzati previo permesso scritto da parte del team dei Servizi informatici.

<u>Accesso a dati conservati in formato digitale</u>:

- Utilizzare delle password per poter accedere a file sensibili.
- Non aggirare sistemi di sicurezza esistenti o livelli di autorizzazione stabiliti.
- Avere un documento che permetta una verifica effettuabile sulle modifiche che sono state apportate ai database o ai documenti che contengono informazioni sensibili.

- Non ostacolare i back-up informatici stabiliti.

Sicurezza di dispositivi portatili:

- Se l'utente è stato autorizzato ad accedere ai sistemi informatici o alle infrastrutture di NEP, è responsabile per la loro salvaguardia e deve fare il possibile per garantire che tali sistemi, non siano utilizzati da persone non autorizzate, che non vengano persi, rubati, danneggiati, specialmente durante viaggi o quando l'utente si trova al di fuori dell'ufficio.
- I dispositivi portatili non devono essere lasciati in auto in nessun momento, soprattutto durante la notte, ma nel caso in cui fosse assolutamente necessario, bisogna assicurarsi che non siano visibili.
- Nel caso in cui i dispositivi portatili dovessero essere utilizzati, per esempio, sui mezzi o in spazi pubblici, tipo lobby di un hotel, bisogna assicurarsi che lo schermo non sia visibile dagli altri passeggeri, e alla luce di quanto richiesto, bisognerà prendere le precauzioni appropriate.
- Nel caso in cui l'utente utilizzi il suo dispositivo portatile per accedere a una rete esterna o appartenente a terzi, per esempio, se si dovesse connettere alla rete internet di un hotel o di un aeroporto, dovrà prendere le precauzione appropriate per assicurarsi che la rete sia sicura. In questo caso, si consiglia di utilizzare una connessione rete fornita da un'azienda riconosciuta e che sia preferibilmente accessibile tramite password anziché con libero accesso. Nel caso ci fossero dei dubbi sulla sicurezza della rete, non bisogna connettersi con il computer.
- Evitare di eludere i software di criptografia o le impostazioni di sicurezza dei dispositivi portatili.
- NEP utilizza una combinazioni delle seguenti impostazioni di sicurezza su dispositivi portatili per assicurare che siano mantenuti sicuri:
    - nome utente/password e PIN;
    - protezione anti-virus;
    - crittografia dei dati;
    - disconnessione dall'account in seguito a diversi tentativi di accesso non andanti a buon fine;
    - dispositivo/applicazione bloccata in seguito a una fase di inattività;
    - account o dispositivo bloccati in seguito a furto/perdita;
    - verifica dell'utilizzo; e
    - cancellazione di contenuti su dispositivi persi o rubati.

Sicurezza sul posto di lavoro di copie cartacee relative ai Dati Personali:

- Assicurarsi che sulla vostra scrivania non ci siano informazioni relative ai Dati Personali o a informazioni aziendali sensibili.

- Non lasciare i Dati Personali o informazioni aziendali sensibili incustodite sulle scrivanie in nessun momento.
- Nel caso in cui si dovessero stampare dei Dati Personali sensibili o delle informazioni aziendali confidenziali e sensibili, assicurarsi di non allontanarsi dalla stampante per evitare che qualcun'altro recuperi i suddetti documenti.
- Non lasciare Dati Personali sensibili o informazioni aziendali confidenziali e sensibili in sale riunioni o in altre aree dell'ufficio, portarli sempre con se e gettarli in modo sicuro se non se ne ha più bisogno. Pulire le lavagne bianche prima di lasciare le sale riunioni, a meno che sia stato richiesto espressamente di non farlo.
- Chiudere a chiave/conservare i Dati Personali sensibili o informazioni aziendali confidenziali e sensibili in un posto sicuro durante la notte, per esempio in un archivio, cassetto che si possono chiudere a chiave o in una stanza con accesso ridotto o in un'area/stanza chiusa a chiave.
- Si prega di seguire le direttive che sono state impartite dal sito operativo o dipartimento locale.

Sicurezza al di fuori del posto di lavoro di copie cartacee relative ai Dati Personali:

- Solo Dati Personali o informazioni aziendali confidenziali e sensibili al di possono essere portati fuori dell'ufficio, solo se strettamente necessario.
- Essere consapevoli della possibilità di perdita o di furto e prendere precauzioni appropriate per assicurare che i Dati Personali o le informazioni aziendali confidenziali e sensibili siano mantenuti al sicuro.
- Non lasciare i Dati Personali o informazioni aziendali confidenziali e sensibili incustoditi in nessun momento sui treni o su qualsiasi altro tipo di trasporto pubblico o in luoghi pubblici. Assicurarsi che le informazioni aziendali sensibili non siano facilmente visibili quando si è in luoghi pubblici.
- Conservate o archiviare Dati Personali o informazioni aziendali confidenziali e sensibili al di fuori dell'ufficio, solo utilizzando un fornitore approvato da NEP, con cui sia stato stabilito un contratto per iscritto.

Utilizzo di dispositivi mobili di conservazione dati:

Dispositivi portatili/amovibili ("**Supporti**") includono tutti quei supporti portatili capaci di conservare, trasferire, modificare o cancellare i dati e che includono (ma non si limitano) i dispositivi portatili, i flash disk, le penne USB, hard drive trasportabili e supporti ottici (CD, DVD, etc.).

- I dati possono essere trasferiti solo dai sistemi informatici NEP ad altri Supporti nel caso in cui ci sia una giustificazione aziendale fondata e solo nel caso in cui le linee guida stabilite da questa Politica e dal team dei Servizi informatici siano rispettate.
- NEP verifica tutti i dati copiati dalla rete per rilevare eventuali trasferimenti di dati non autorizzati e per evitare violazioni della sicurezza.
- Lo scambio di dati sia internamente, che con parti esterne, deve sempre essere effettuato tramite i sistemi di informazione NEP, quali le email o tramite aree previste per la condivisione di dati. L'utilizzo di Supporti per il trasferimento di dati dovrà essere usato solo nell'evenienza in cui tutte le altre opzioni siano state esaurite.

- Tutti i Supporti che vengono trasferiti fisicamente tra NEP e/o un cliente, dovrebbero essere spediti tramite una consegna speciale (per garantire che il Supporto possa essere seguito e recuperato in caso di perdita).

- Prima di utilizzare i Supporti, si prega di tenere conto dei punti seguenti:
    - utilizzare solo Supporti che sono stati acquistati o autorizzati dai Servizi di Informazione NEP e che siano criptati;
    - i supporti devono poter essere tracciabili per assicurare che arrivino alla destinazione voluta;
    - i supporti devono essere analizzati tramite l'antivirus fornito dai Servizi di Informazione NEP prima di essere utilizzati, non devono presentare malware o essere stati infettati da virus e non devono essere utilizzati se viene riscontrata una possibile infezione;
    - conservare solo i dati che sono assolutamente necessari, per esempio, si prega di non scaricare un database intero se soltanto piccole sezioni sono richieste;
    - verificare che i Supporti di archiviazione mobile possano codificare i Dati Personali;
    - assicurarsi che i file salvati sui Supporti siano protetti con una password e che la password sia stata inviata separatamente al Supporto criptato;
    - cancellare immediatamente i dati dal Supporto quando non sono più richiesti; e
    - i Supporti non riutilizzabili devono essere gettati/distrutti in modo corretto alla fine del loro ciclo di vita, rispettando le raccomandazioni del team dei Servizi di Informazione.

<u>Restrizioni sull'utilizzo di dispositivi e software non autorizzati</u>:

- Non scaricare software senza licenza, software appartenenti a terzi, software accessibili gratuitamente o qualsiasi altro tipo di software sul computer o su altri dispositivi informatici poiché potrebbero contenere virus o altri codici nocivi che potrebbero violare la sicurezza dei sistemi NEP.

<u>Accessibilità terzi</u>:

- NEP è responsabile per i comportamenti o le omissioni da parte dei suoi fornitori e di appaltatori che possono accedere o trattare i Dati Personali per suo conto. Se vengono assunti appaltatori, consulenti o personale temporaneo e se gli stessi hanno accesso ai sistemi NEP e/o a Dati Personali, devono innanzitutto firmare un accordo contenente una serie di provvedimenti che riguardano la protezione dei Dati Personali NEP, per esempio, confidenzialità e sicurezza. Si consiglia di contattare il Responsabile locale per la Protezione dei Dati per ricevere delle linee guida sui provvedimenti richiesti.
- In particolare, qualsiasi progetto che preveda che terzi o fornitori esterni abbiano accesso ai sistemi NEP, richiederà una valutazione dei rischi e un'aggiunta ai termini contrattuali relativa alla sicurezza.
- Tutte le modifiche effettuate da terzi o fornitori esterni aventi accesso alla rete di NEP, devono essere riviste e documentate per garantire che il livello di sicurezza sia mantenuto.

- Se il rapporto con terzi o con fornitori di servizi esterni non fosse più richiesto, la possibilità di connettersi deve essere conclusa e tutti i Dati Personali ottenuti da terzi o dai fornitori di servizi esterni, devono essere riconsegnati o distrutti secondo i termini contrattuali.
- A tutti i fornitori di servizi esterni e a terzi, viene richiesto di informare NEP, tramite il loro metodo di comunicazione principale, relativamente a tutte le informazioni relative ad eventuali incidenti sulla sicurezza che possano avere riscontrato direttamente o che siano stati riscontrati dai loro clienti.

Back-up dei Dati Personali:

- Quando possibile i dati dovrebbero essere conservati in un archivio in rete, in quanto è possibile effettuarne facilmente il back-up tramite processi automatizzati. Dispositivi mobili, come per esempio penne USB e CD non devono essere utilizzati per conservare informazioni aziendali critiche poiché non si può effettuare il back-up e di conseguenza tali informazioni non potranno essere recuperate in caso di eliminazione accidentale o di danneggiamento.

Smaltimento dei Dati Personali:

I Dati Personali in versione cartacea devano, laddove possibile, essere smantellati utilizzando dei cestini appositi per lo smaltimento di Dati Personali o il distruggi documenti.

- Assicurarsi che tutti gli hardware, dispositivi mobili, dispositivi di conservazione mobile o altre apparecchiature siano state adeguatamente pulite prima di smantellare i Dati Personali. I dispositivi non riutilizzabili, quali i CD-ROM, devono essere smaltiti o distrutti alla fine del loro ciclo di vita. Contattare il team dei Servizi di Informazione per assicurarsi che questa procedura si effettuata in modo corretto.

Utilizzo delle email e del sistema:

- Non cercare di eludere l'antivirus, per esempio, disattivandolo.
- I dipendenti dovranno fare attenzione quando aprono email provenienti da fonti esterne sconosciute o dove, per qualsiasi ragione, un'email appaia sospetta (per esempio se il nome termina con .exe).
- Il team dei Servizi di Informazione deve essere immediatamente informato se un virus sospetto è stato ricevuto o identificato.
- NEP si riserva il diritto di bloccare la possibilità di allegare file alle email per permettere un uso efficace dei sistemi informatici NEP e per rispettare la presente Politica.
- NEP si riserva inoltre il diritto di non inviare (né in entrata e né in uscita) alcun messaggio di posta elettronica, se si sospetta che un virus sia allegato.
- NEP permette di utilizzare in modo occasionale internet, le email, il telefono per inviare email personali, navigare su internet ed effettuare telefonate personali a determinate condizioni, come previsto qui di seguito. L'uso personale è un privilegio non un diritto. Non si deve né abusare, né farne un uso eccessivo e NEP si riserva il diritto di rettificare l'autorizzazione in

qualsiasi momento. NEP si riserva il diritto di ridurre o di limitare l'accesso a certi numeri di telefono o ad alcuni siti internet, se considera che l'utilizzo personale abbia superato il limite. Le seguenti condizioni devono essere rispettate affinché l'utilizzo personale possa continuare:

  - l'utilizzo deve essere minimo e deve principalmente avvenire al di fuori dell'orario di lavoro;
  - l'utilizzo non deve interferire con gli impegni aziendali o dell'ufficio; e
  - l'utilizzo non deve rappresentare alcun genere di costo per NEP.
- Tutte le email inerenti ad attività aziendali devono essere approvate dal sistema di gestione delle email aziendale.

Contatti dei clienti:

- Copie di agende telefoniche o altri documenti o dispositivi che contengono informazioni relativi a contatti aziendali non devono essere lasciati incustoditi.
- Se i contatti aziendali vengono conservati in formato digitale, bisogna conservarli in un'area sicura della rete NEP.

11. Segnalazione di sospette violazioni della sicurezza dei dati

Una violazione dei dati può accadere in relazione a o in seguito di uno degli eventi seguenti (questa lista non è esaustiva):

- furto di dati (incluse copie cartacee) o di dispositivi (computer portatili, telefoni cellulari, penne USB, CD-ROM, etc.) sui quali i dati sono stati salvati;
- l'utente non è sufficiente informato/mancanza di formazione;
- accesso o copie non autorizzate;
- classificazione/marcatura/etichettatura della sicurezza non corretta;
- metodo di trasmissione non sicuro;
- utilizzo di dispositivi che non sono stati controllati o autorizzati;
- perdita, o possibile perdita, di dispositivi, supporti o apparecchi;
- perdita o possibile perdita del backup dei dispositivi;
- conservazione inadeguata delle informazioni;
- dirottamento/deviazione dei Dati Personali;
- metodo di smaltimento dei dati o dei supporti incorretto;
- hackeraggio/intercettazioni;

- registrazioni nascoste/spionaggio;
- rilascio inappropriato al pubblico dominio;
- accesso da parte di manutentori/fornitori di servizi esterni non supervisionati;
- controlli di accesso non adeguati che permettono un utilizzo non autorizzato a membri del personale o altre persone; o
- informazioni ottenute ingannando NEP.

Se l'utente dovesse venire a conoscenza della violazione sulla sicurezza dei Dati Personali (o di altri dati) o se sospetta che sia avvenuta, bisognerà segnalarlo immediatamente al Responsabile per la Protezione dei Dati e al responsabile diretto che deve informare le autorità competenti in materia di protezione dei dati e la persona i cui dati sono stati violati. È responsabilità dell'utente di assicurarsi che la segnalazione sia stata ricevuta e che il Responsabile per la Protezione dei Dati e il responsabile diretto siano immediatamente messi a conoscenza che la segnalazione è stata inviata (inviare un'email o lasciare un messaggio vocale potrebbe risultare insufficiente. Se non si è sicuri che il destinatario abbia ricevuto il messaggio, sempre verificare).

L'utente dovrà cercare di fornire più informazioni possibili (incluse le informazioni sopra citate, ma non solo):

- la natura dei dati coinvolti (se si stratta di dati sensibili o di altro genere);
- quando è avvenuta la violazione;
- come è avvenuta la violazione (se per esempio i dati sono stati rubati o persi o se si sospetta ci sia stato un accesso non autorizzato);
- se i dati sono stati danneggiati o corrotti, in che modo sono stati danneggiati o corrotti;
- quanti Dati Personali di individui sono stata interessati da questa violazione;
- q quali individui appartengono i dati che sono stati perduti (per esempio se si tratta di documenti appartenenti al personale, ai clienti, o ai fornitori);
- misure che sono o che devono essere intraprese per evitare ulteriori problemi, nel caso in cui si tratti di una violazione ricorrente, o se ulteriori dati sono stati colpiti; e
- se esiste un qualsivoglia impegno contrattuale da parte di terzi in merito alla sicurezza dei Dati Personali (per esempio i clienti NEP).

Successivamente l'utente dovrà partecipare ad arrestare o a mitigare la violazione dei dati personali.

12. Assicurare gli individui su come verranno utilizzati i loro dati da NEP

In alcune circostanze il consenso esplicito degli individui dovrà essere richiesto. NEP dispone di dichiarazioni sulla privacy standard e di clausole che sono state integrate ai suoi contratti standard per assicurare che questo requisito venga rispetto e per fornire delle direttive a coloro che vogliono sapere quando deve essere richiesto un consenso esplicito.

13. Assicurare che i Dati Personali siano corretti e aggiornati

Tutte le inesattezze relative ai Dati Personali in possesso di NEP devono essere corrette da un membro del personale su tutti i sistemi interessati. Eventuali aggiornamenti o cambiamenti delle informazioni fornite da un individuo devono essere riportati anche sulle registrazioni di NEP.

Le persone interessate devono essere informate del loro diritto di accedere, correggere, cancellare o limitare il trattamento dei Dati Personali che sono stati raccolti.

14. Smaltimento sicuro dei Dati Personali

Se i Dati Personali non sono più richiesti, bisogna assicurarsi che vengano smaltiti con attenzione e in modo sicuro.

Se un membro del personale riceve una richiesta di informazioni in riferimento a una qualsiasi legge sulla Protezione dei Dati, si prega di contattare immediatamente il Responsabile locale per la Protezione dei Dati, per garantire che l'informazione sia gestita in modo corretto ed entro i tempi previsti.

15. Valutazione d'impatto sulla vita privata

Nel caso in cui nuovi procedimenti, politiche o procedure, stiano per essere implementati, o che un nuovo progetto stia per essere lanciato o che nuovi sistemi stiano per essere acquistati, che includono la gestione o il trasferimento di una quantità importante di Dati Personali o che potrebbe avere un impatto pratico sulla vita privata o sulla sicurezza dei Dati Personali trattati da o a conto di NEP, allora bisognerà eseguire una Valutazione d'impatto sulla vita privata ("**PIA**"). Si prega di fare riferimento alle linee guida PIA di NEP. Questo può anche accadere nel caso in cui si stesse delocalizzando una particolare attività o servizio o nel caso di un'acquisizione significativa.

16. Formazione

La partecipazione a tutti i corsi che riguardano la protezione e la gestione dei Dati Personali ai quali NEP ha chiesto di partecipare è obbligatoria. Queste formazioni includono corsi fuori che possono essere seguiti in ufficio e corsi online.

17. Consulenza esterna da parte dell'autorità locale responsabile della protezione dei dati

Sul sito del Comitato europeo per la protezione dei dati, sul sito ICO (Regno Unito) e sui siti di altre autorità per la protezione dei dati, sono disponibili un certo numero di linee guide molto utili.

18. Protezione dei dati e azioni disciplinari

Se un individuo contravviene (o è sospettato di avere contravvenuto) a un qualsiasi aspetto della presente Politica, delle azioni disciplinari appropriate possono essere intraprese conformemente alla procedura disciplinare applicabile.

A seconda della gravità del comportamento, l'azione disciplinare può comportare il licenziamento senza preavviso.

NEP si riserva il diritto di intraprendere qualsiasi altra azione nei confronti di un individuo che sia stato appena licenziato (inclusa la revoca del diritto di accesso autorizzato ai Dati Personali) in base alle circostanze.

Nel caso in cui un individuo dovesse avere dei dubbi sul come stia trattando i Dati Personali, in modo giusto e legale, può contattare il team responsabile per la Protezione dei Dati, prima di iniziare qualsiasi tipo di manovra.

19. Verifica e revisione della presente Politica

La presente Politica viene revisionata periodicamente. Gli utenti saranno avvertiti nel caso di eventuali cambiamenti significativi, che verranno apportati alla presente Politica, direttamente dal sito internet di NEP.

Approvazione

L'attuazione della presente Politica è stata approvata da:

_____	_____
Amministratore delegato	Data
_____	_____
Responsabile Affari legali e Responsabile Conformità	Data
_____	_____
Vice Presidente Senior del dipartimento Risorse umane	Data

Cronologia revisioni

Data	**Riepilogo revisioni** (inizia con il numero/titolo della sezione)
1 maggio 2018	Politica in vigore