PROCEDURE OPERATIVE PRIVACY
DI LOCATELLI SALINE DI VOLTERRA S.R.L.
ADOTTATE IN DATA 09/01/2019
AI SENSI DELL'ART. 32 DEL REG. EU N. 679/2016 (C.D. "GDPR")

Si premette che la Società ha individuato due referenti ai quali sono state demandate funzioni di coordinamento e assistenza per i singoli incaricati.

Sono stati, in particolare, individuati:

- un referente interno per i trattamenti concernenti le Risorse Umane (ivi compresi quelli inerenti i dati dei tirocinanti ed i dati dei candidati);
- un referente interno per i trattamenti concernenti le attività commerciali (clienti, fornitori e agenti).

Ciascun dipendente, autorizzato secondo le lettere di incarico, è considerato un "**Incaricato**" al trattamento ai sensi del GDPR.

1. Regolamento informatico

1.1. Principi di Comportamento

Nell'utilizzo dei sistemi informatici, ciascun Incaricato è tenuto al rispetto delle previsioni normative e dei protocolli aziendali.
Sono strumenti di lavoro tutte le dotazioni informatiche fornite dalla Società ivi compresi telefoni cellulari, tablet, pec, caselle di posta elettronica, dispositivi di archiviazione di vario tipo nonché i prodotti software e le applicazioni installate su ciascuno degli strumenti aziendali.
Le dotazioni aziendali possono essere utilizzate solo ed esclusivamente con finalità lavorativa essendo l'uso personale vietato in quanto, tra l'altro, facilita la diffusione di virus e l'accesso non autorizzato alla rete aziendale.
Gli Incaricati devono utilizzare gli strumenti informatici attenendosi alle prescrizioni contenute nelle presenti procedure e nei limiti di quanto previsto dalle lettere di incarico ai sensi del reg. EU n. 679/2016.
Nell'utilizzo degli strumenti aziendali ciascun Incaricato è tenuto al rispetto dei seguenti principi:

- è vietato l'accesso a sistemi informatici di terzi senza le necessarie autorizzazioni;
- è vietato aggirare o tentare di aggirare sistemi di protezione;
- le informazioni contenute negli strumenti informatici aziendali devono considerarsi riservate e non possono, pertanto, essere divulgate a terzi.

1.2 Credenziali di autenticazione

L'accesso al proprio pc da parte degli Incaricati deve avvenire mediante credenziali di accesso personali, soggette a variazione trimestrale, custodite da parte di ciascun incaricato al fine di impedirne la conoscenza a terzi e comunicate all'Amministratore di Sistema che ne custodisce copia.
Le credenziali sono consegnate, al primo utilizzo, dall'Amministratore di Sistema e sono costituite da un user ID e da una password che dovrà essere costituita dal nome utente PC ed un progressivo numerico che si incrementa periodicamente.
È vietato l'utilizzo di credenziali di autenticazione di terzi.
La visione delle cartelle del server aziendale è stata abilitata ai soli soggetti con mansioni che necessitano la consultazione del contenuto delle cartelle medesime.
Ciascun Incaricato è tenuto al rispetto delle abilitazioni al medesimo conferite, coerenti con le mansioni svolte.

Nel caso sorga la necessità di accedere a documentazione posizionata su cartelle non abilitate, l'Incaricato dovrà fare richiesta al Referente Interno competente, che si rivolgerà per la decisione all'organo amministrativo.

1.3 Regole di condotta

Ciascun Incaricato è tenuto al rispetto delle seguenti regole di condotta:

1. proteggere gli strumenti di lavoro anche attraverso l'esecuzione dei suggeriti aggiornamenti software onde evitare o comunque ridurre il rischio di intrusione;
2. chiudere, in caso di allontanamento dalla propria postazione, le sessioni di lavoro in corso;
3. non è consentito scaricare o installare programmi non autorizzati o in violazione delle procedure aziendali;
4. astenersi dal rimuovere o comunque modificare le componenti hardware degli strumenti di lavoro;
5. proteggere gli strumenti informatici per l'utilizzo in mobilità da possibili furti o smarrimenti adottando le necessarie cautele nel loro utilizzo e nel loro trasporto evitando di lasciarli incustoditi e/o comunque esposti al rischio di sottrazione;
6. utilizzare connessioni esterne solo se dotate del protocollo VPNM
7. eseguire le necessarie copie di backup degli strumenti in dotazione che non siano connessi in rete;
8. adottare le cautele comunque necessarie al fine di proteggere il patrimonio aziendale e le informazioni contenute nei dispositivi;
9. non è ammesso l'uso di periferiche mobili (dischi rimovibili, USB) o altri supporti mobili (CD, DVD) per accedere, memorizzare, scaricare o distribuire informazioni proprietarie;
10. l'utilizzo di periferiche mobili o altri supporti è consentito solo dietro autorizzazione dell'organo amministrativo;
11. non è consentito l'utilizzo di periferiche o supporti personali;
12. non è consentito l'utilizzo di internet con finalità diverse da quelle lavorative ed è conseguentemente vietato, a mero titolo esemplificativo e non esaustivo e salva autorizzazione in senso contrario del datore di lavoro: (i) l'installazione di software gratuiti o shareware; (ii) l'esecuzione di transazioni finanziarie ivi comprese quelle tramite home-banking o acquisti online; (iii) la registrazione a siti non attinenti l'attività lavorativa; (iv) utilizzo dei social network al di fuori dei soggetti espressamente autorizzati ai fini dello svolgimento delle loro mansioni;
13. astenersi dal conservare file personali sulla rete aziendale e sugli strumenti informatici aziendali.

Ciascun Incaricato è responsabile delle violazioni delle prescrizioni qui contenute nonché delle conseguenze, anche patrimoniali, in capo alla Società derivanti dalle violazioni delle presenti regole.

1.4 Smarrimento di strumenti informatici e segnalazioni di intrusioni o compromissioni di strumenti

Ciascun Incaricato deve dare tempestiva informazione all'Amministratore di Sistema, ai Referenti Interni ed all'organo amministrativo nei seguenti casi:

1. smarrimento di strumenti informatici, dispositivi mobili, dispositivi di archiviazione o, in ogni caso di supporti o strumenti aziendali e personali che contengano informazioni e dati aziendali;
2. segnalazione da parte dei software antivirus in dotazione sugli strumenti informatici in uso di violazioni o di presenza di virus;
3. altri eventi o segnalazioni che evidenzino un rischio di compromissione, anche potenziale, della rete aziendale e/o di strumenti informatici aziendale.

L'organo amministrativo attiva tempestivamente le procedure necessarie al fine di impedire l'accesso da parte di terzi dei contenuti presenti nello strumento informatico perduto.

Qualsiasi ritardo nella segnalazione dello smarrimento di strumenti informatici è da ritenersi violazione della presente procedura.

1.5 Cessazione del rapporto di lavoro

In caso di cessazione per qualsiasi motivo del rapporto di lavoro, l'Incaricato dovrà mettere a disposizione della Società e/o restituire qualsiasi risorsa gli fosse stata assegnata, sia con riferimento alle attrezzature informatiche sia, più in generale, al patrimonio informativo a lui fornito e/o utilizzato ovvero che il medesimo abbia raccolto o contribuito a costituire e che rivesta interesse aziendale.

A seguito della cessazione del rapporto:

- l'Incaricato potrà cancellare le informazioni di "natura aziendale" presenti nelle postazioni di lavoro e/o nei repository o cartelle condivise "solo ed esclusivamente" dietro esplicita autorizzazione del Referente Interno competente;
- qualora l'Incaricato dovesse lasciare sulle postazioni di lavoro e/o repository o cartelle condivise informazioni o dati personali propri e comunque di interesse non aziendale, queste saranno rimosse e cancellate senza che sia ipotizzabile alcuna responsabilità in capo alla Società (sul punto vedere il Provvedimento del Garante Privacy del 22 aprile 2010).

2. Risorse Umane

2.1 Dati inerenti i lavoratori

I documenti cartacei contenenti informazioni inerenti il rapporto di lavoro (buste paga, contratti di lavoro e altro) sono conservati in armadio accessibile ai soli addetti all'amministrazione.

La rilevazione delle presenze dei dipendenti avviene attraverso un timbratore, il Referente Interno HR invia il foglio presenze allo studio paghe, il quale elabora le buste paga che vengono ritirate personalmente in busta chiusa da un componente del CdA o da un suo incaricato che provvede, relativamente alla sede di Bolgare, a consegnarle alla responsabile amministrativa. Inoltre lo studio paghe invia via mail le buste paga in formato PDF alla responsabile amministrativa, che le salva su una cartella accessibile soltanto alla medesima.

I documenti contenenti i dati dei lavoratori sono conservati in armadi chiusi a chiave accessibili soltanto agli addetti all'amministrazione.

Per quanto riguarda la sede di Volterra, un dipendente invia mensilmente via mail il foglio presenze allo studio paghe, il quale elabora le buste paga che vengono ritirate personalmente in busta chiusa da un componente del CdA o da un suo incaricato che provvede a consegnarle in busta chiusa ai dipendenti della sede di Volterra.

Nel caso in cui sia necessario effettuare trasmissioni o riproduzione di documenti contenenti dati personali dei lavoratori, l'Incaricato adotta le seguenti cautele:

- non lasciare incustoditi presso fax, stampanti e fotocopiatrici documenti contenenti dati personali;
- in caso di trasmissione via fax di documenti contenenti dati personali verificare, eventualmente per via telefonica, l'avvenuta ricezione del fax e, una volta trasmessi, ritirarli immediatamente.

I dati sono conservati per 11 anni dalla cessazione del rapporto dopodiché sono cancellati.

2.2 Dati inerenti i tirocinanti

La funzione amministrazione è altresì responsabile del trattamento dei dati inerenti i soggetti ospitati nell'ambito di progetti di tirocinio.

L'Incaricato è tenuto a verificare i dati del tirocinante ed a fornire al medesimo la necessaria informativa al trattamento dei dati richiedendo al tirocinante di apporre la sottoscrizione per ricevuta sull'informativa, conservando copia dell'informativa sottoscritta per ricevuta.

In caso di minori di età si renderà necessario l'espressione del consenso da parte dei genitori, che dovrà essere verificata dall'incaricato.

La documentazione viene archiviata e gestita con le medesime modalità inerenti la documentazione relativa ai lavoratori.
I dati sono conservati per 11 anni dalla cessazione del tirocinio dopodiché sono cancellati.

2.3 Dati inerenti i candidati

L'amministrazione è responsabile della gestione dei Curricula ricevuti tramite email o cartacei.
Nel caso sia possibile l'Incaricato fornisce al candidato l'informativa sul trattamento dei dati.
La documentazione viene archiviata e gestita con le medesime modalità inerenti la documentazione relativa ai lavoratori.
I dati sono conservati per 12 mesi dalla ricezione del Curriculum dopodiché sono cancellati.

3. Amministrazione

Gli addetti all'ufficio amministrazione inseriscono i dati di fornitori e controparti contrattuali nel programma gestionale in uso verificando la rispondenza dei dati con i documenti consegnati dal cliente e dal fornitore.
In occasione della prima consegna dei dati, l'amministrazione consegna alla controparte contrattuale l'informativa privacy a mani, richiedendo di apporre la sottoscrizione per ricevuta sull'informativa, ovvero la trasmette con mezzi che forniscano prova dell'avvenuta ricevuta.
Le copie delle informative sottoscritte per ricevuta e di quelle inviate sono conservate – queste ultime con la prova dell'avvenuta consegna – dall'ufficio amministrazione.
La documentazione viene archiviata in formato cartaceo in armadio accessibile ai soli addetti dell'ufficio amministrazione e dell'ufficio commerciale.
L'accesso agli archivi contenenti i dati di clienti e fornitori è controllato dai componenti dell'ufficio amministrazione.
Nel caso in cui sia necessario effettuare trasmissioni o riproduzione di documenti contenenti dati personali dei clienti e dei fornitori l'Incaricato adotta le seguenti cautele:

- non lasciare incustoditi presso fax, stampanti e fotocopiatrici documenti contenenti dati personali;
- in caso di trasmissione via fax di documenti contenenti dati personali verificare, eventualmente per via telefonica, l'avvenuta ricezione del fax e, una volta trasmessi ritirarli immediatamente.

I dati sono conservati per 11 anni dopodiché sono cancellati.

4. Data Breach

Qualsiasi Incaricato che riceva una segnalazione di sospetta o avvenuta violazione dei dati personali, ha la responsabilità di portare l'avvenimento immediatamente all'attenzione di un Referente Interno.
Di seguito si riportano alcuni eventi al verificarsi dei quali è necessario che sia immediatamente notificato l'accaduto al Referente Interno:

1. perdita o furto di pc o smartphone aziendale;
2. perdita di supporti mobili quali pen-drive usb o hard disk;
3. perdita di faldoni cartacei o altra documentazione aziendale;
4. invio erroneo di comunicazioni verso l'esterno;
5. furti in azienda;
6. attacchi informatici ai sistemi aziendali.

La violazione dei dati può consistere in:

- "*violazione della riservatezza*", in caso di divulgazione o accesso accidentale ai dati personali;
- "*perdita della disponibilità*", in caso di perdita o distruzione dei dati personali (accidentale o non autorizzata);
- "*violazione dell'integrità*", in caso di alterazione non autorizzata o accidentale dei dati personali.

Nel caso di avvenuta violazione dei dati, il Referente Interno che ha ricevuto la segnalazione dovrà verificare se sussistono i presupposti per dar corso:

1. alla notifica al garante dell'avvenuta violazione;
2. alla notifica agli interessati dell'avvenuta violazione.

Il Referente Interno dovrà quindi riferire immediatamente all'organo amministrativo che, con l'ausilio di un consulente e del Referente Interno, e tenendo conto delle tempistiche previste dal GDPR per la notifica del "Data Breach", tempistiche che prevedono 72 ore dalla conoscenza della violazione, dovrà provvedere a dar corso alle necessarie attività.

5. Esercizio di diritti da parte degli interessati

Nel caso di esercizio da parte degli interessati, siano gli stessi lavoratori, clienti, fornitori, candidati o tirocinanti, ovvero altre categorie non censiste di interessati, l'Incaricato che venga a conoscenza della richiesta di esercizio da parte dell'interessato è tenuto a dare immediata comunicazione al Referente Interno. Quest'ultimo verifica la richiesta proveniente dall'interessato e, confrontandosi con il consulente, valuta se sussistono i presupposti per l'esercizio del diritto enunciato dall'interessato.
La richiesta dell'interessato dovrà essere riscontrata entro 20 giorni dalla richiesta.

6. Violazioni

È fatto obbligo a tutti gli Incaricati di osservare le presente procedure.
Il mancato rispetto o la violazione delle regole sopra ricordate possono di per sé considerarsi contrari ai doveri di diligenza e fedeltà previsti dagli artt. 2104 e 2105 del Codice civile e potrà comportare l'applicazione al personale dipendente di sanzioni disciplinari in base a quanto previsto dall'art. 7 della L. 20 maggio 1970, n. 300 (Statuto dei Lavoratori), di quelle previste dal vigente CCNL nonché il ricorso alle opportune azioni civili e penali previste.
In caso di violazione accertata delle previsioni delle presenti procedure da parte di un Incaricato, nel rispetto della normativa sopra richiamata, verrà avviata la procedura prevista per l'applicazione delle sanzioni disciplinari che sarà graduata in funzione della violazione commessa come previsto dal CCNL.
In presenza di violazioni accertate da parte degli Incaricati delle regole e delle prescrizioni contenute nelle presente procedure potrà essere applicata, con immediatezza ed in attesa di ulteriori verifiche, una limitazione dell'utilizzo degli strumenti di lavoro attraverso azioni di sospensione, blocco o limitazione degli accessi dell'account individuale al fine di proteggere l'integrità, la sicurezza e/o la funzionalità del sistema informatico aziendale e, complessivamente, delle attività operative aziendali.