POLICY PER IL TRATTAMENTO DEI DATI

PHONIKA S.P.A.

SOMMARIO

1.0 PREMESSA

La società PHONIKA SPA., con sede in Piazza Alfieri 17 – 14100 ASTI, P.IVA: 01403360058, in qualità Titolare del trattamento dei dati e Responsabile del trattamento dei dati per le proprie committenti, ha inteso istituire la presente Policy Privacy Aziendale al fine di garantire corrette operazioni di trattamento da parte dei propri dipendenti/collaboratori nello svolgimento dell'attività lavorativa prestata.

Il presente documento è stato redatto nel rispetto di quanto disposto:

- dal Regolamento Generale sulla Protezione dei Dati (REGOLAMENTO UE 2016/679),
- dalle "Linee guida del Garante per posta elettronica e internet" (Gazzetta Ufficiale n. 58 del 10 marzo 2007);
- dall'Art. 4 della Legge 20 Maggio 1970, n. 300 (Statuto dei Lavoratori) – come modificato dal Decreto Legislativo 14 settembre 2015, n. 151 (Disposizioni di razionalizzazione e semplificazione delle procedure e degli adempimenti a carico di cittadini e imprese e altre disposizioni in materia di rapporto di lavoro e pari opportunità, in attuazione della legge 10 dicembre 2014, n. 183).
- dalle prescrizioni del provvedimento dell'Autorità Garante Privacy del 30 novembre 2005 "Liceità, correttezza e pertinenza nell'attività di recupero crediti";
- dalle indicazioni del "Codice di condotta per i processi di gestione e tutela del credito" sottoscritto dal Forum Unirec-Consumatori.

Le regole riportate nella presente POLICY PRIVACY AZIENDALE si applicano indistintamente a tutti i dipendenti e collaboratori dell'azienda a prescindere dal rapporto contrattuale con la stessa intrattenuto (a titolo di esempio non esaustivo, lavoratori somministrati,

collaboratori a progetto, in stage/tirocinio, eventuali liberi professionisti/lavoratori autonomi, etc…).

2. LA SOCIETA'

Phonika S.p.A. opera, a livello nazionale, nell'ambito del settore terziario, offrendo servizi legati alla gestione del credito a favore di Banche, Finanziarie e Aziende Commerciali.

2.1 AREE DI OPERATIVITA' DI PHONIKA S.P.A.

La società consta delle seguenti Aree di operatività:

- Direzione;
- Customer Service e Reception;
- Contabilità e fatturazione;
- Compliance e privacy;
- Risorse umane;
- Operation.

2.2 TIPOLOGIA DEI DATI TRATTATI

- Dati comuni e particolari (essenzialmente di natura sanitaria e giudiziaria) relativi al personale ed ai collaboratori;
- Dati comuni relativi ai clienti;
- Dati comuni relativi a fornitori;
- Dati relativi allo svolgimento di attività economiche e commerciali;
- Dati comuni di terzi, forniti dai clienti per l'espletamento degli incarichi affidati alla società, compresi i dati sul patrimonio e sulla situazione economica, o necessari a fini fiscali o afferenti alla reperibilità ed alla corrispondenza con gli stessi, o per atti giudiziari.

2.3 MISURE LOGICHE DI SICUREZZA

Per il trattamento effettuato con sistemi informatici la Società attua le seguenti misure:

- sistema di autentificazione informatica volto ad accertare l'identità delle persone che hanno accesso agli strumenti elettronici;
- le Password sono gestite secondo quanto previsto nel previgente allegato B del D.Lgs. 196/2003;
- è stato individuato e nominato per iscritto l'Amministratore di Sistema a cui spetta la custodia, in un luogo sicuro, della password per l'accesso ai dati archiviati nelle singole postazioni;
- protezione di strumenti e dati da malfunzionamenti e attacchi informatici attraverso programmi antivirus; gli aggiornamenti sono pianificati automaticamente dall'antivirus e le licenze sono regolarmente rinnovate alla scadenza;
- installazione di un firewall atto ad evitare intrusioni ai server dall'esterno;
- tutti i software utilizzati all'interno della Società sono protetti da password;
- predisposizione di un Business Continuity plan informatico e di un piano di Disaster Recovery volta a contrastare eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ...), nonché dolosi, accidentali o dovuti ad incuria.

2.4 STRUTTURA INTERNA IN AMBITO PRIVACY

Allo scopo di fornire supporto all'area operation dell'azienda, anche con riferimento alle problematiche che potrebbero derivare dal trattamento dei dati personali, è stato istituito un apposito ufficio denominato "Compliance e privacy" coadiuvato, in caso di particolari tematiche, dal DPO incaricato.

In particolare l'ufficio svolge due funzioni: da un lato si pone quale interfaccia degli interessati che abbiano indirizzato un reclamo o abbiano esercitato i diritti di cui agli artt. 15-20 GDPR alla società, d'altro lato, proprio grazie all'esame delle istanze/reclami pervenuti, è in grado di offrire supporto all'operation nell'identificare eventuali criticità presenti in procedure e processi.

3. IL TRATTAMENTO NEL RECUPERO CREDITI

Nell'esecuzione dei propri compiti, gli operatori di Phonika S.p.A. addetti al servizio di recupero crediti (di qui in avanti i "Soggetti Designati"), devono rigidamente attenersi alle seguenti istruzioni, allo scopo di garantire la legittimità delle operazioni di trattamenti dei dati personali degli interessati coinvolti.

I Soggetti Designati non possono comunicare e/o diffondere i dati personali trattati in esecuzione dei compiti ricevuti, senza la preventiva autorizzazione del Team Leader. Nessuna comunicazione di dati all'esterno della struttura può avere luogo in assenza di autorizzazione proveniente direttamente dall'organo amministrativo. Anche tra colleghi i dati possono essere comunicati solo per l'espletamento dei relativi incarichi.

I Soggetti Designati non possono effettuare copie di dati e/o programmi al di fuori di quanto espressamente previsto dalle procedure interne di salvataggio dei dati.

I Soggetti Designati possono utilizzare esclusivamente gli strumenti forniti e/o preventivamente autorizzati dalla società. Tali strumenti devono essere esclusivamente utilizzati per svolgere le proprie mansioni.

I dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»).

I Soggetti Designati devono cercare un confronto diretto con il Consumatore/Debitore e verificarne l'identità, pur nei limiti dettati dalla modalità di contatto prescelta, prima di affrontare le ragioni del debito insoluto.

Nella gestione dei mandati, qualora I Soggetti Designati non riescano a stabilire un confronto diretto con il Consumatore/Debitore ed entrino in

contatto con soggetti terzi, dovranno operare secondo i principi definiti nel Provvedimento del Garante Privacy del 30 novembre 2005.

In tali circostanze, I Soggetti Designati non possono fornire "ingiustificatamente" a soggetti terzi informazioni relative allo stato di inadempimento in cui versa il Consumatore/Debitore .

I Soggetti Designati, pertanto, non possono confrontarsi con soggetti terzi, estranei al rapporto contrattuale, se non per legittimi motivi e sempre con l'esclusione dei minori.

Si considera effettuata per legittimi motivi:

a) la comunicazione di informazioni riservate a soggetti terzi i quali si dimostrino già a conoscenza delle circostanze oggetto di mandato e si rendano disponibili a definire la posizione per conto del Consumatore/Debitore assente;

b) la comunicazione di informazioni riservate a soggetti terzi che si dichiarino espressamente delegati dal Consumatore/Debitore a gestire le sue vicende contrattuali.

Qualora il terzo, dopo la presentazione dell'Incaricato secondo le modalità indicate nel presente paragrafo, si dimostri già a conoscenza del debito e domandi di poterlo trattare per conto del Consumatore/Debitore, dovranno essere adottate le stesse cautele ed i medesimi adempimenti previsti a tutela del Consumatore/Debitore.

Qualunque contatto con soggetti formalmente estranei rispetto all'obbligazione oggetto di mandato, in ogni caso, può avere luogo unicamente:

a) in via subordinata, considerata la non immediata reperibilità del Consumatore/Debitore ai recapiti forniti;

b) preservando sempre la dignità e l'onorabilità del Consumatore/Debitore stesso.

Durante ogni contatto, i Soggetti Designati devono presentarsi comunicando il proprio nome e cognome, il luogo dal quale chiamano ed un recapito cui essere ricontattati.
Nel descrivere, inoltre, le ragioni della ricerca, i Soggetti Designati devono limitarsi a rappresentare che la loro attività consiste nel fornire comunicazioni commerciali/amministrative, per conto del Committente/ Creditore, e che le stesse possono essere rilasciate unicamente in favore del destinatario.
Qualora il Consumatore/Debitore non risulti contattabile ai recapiti forniti dal Committente/Creditore, potranno essere espletate attività di ricerca attraverso banche dati pubbliche/pubblici registri, fonti terze autorizzate e informazioni raccolte nel normale svolgimento dell'incarico ricevuto.
In tali circostanze i Soggetti Designati devono:

- verificare, al primo contatto utile, la disponibilità del Consumatore/Debitore ad essere ricontattato al medesimo recapito;
- in caso di risposta negativa, chiedere che sia il Consumatore/Debitore medesimo ad indicare quali recapiti utilizzare per i successivi contatti.

In ogni caso, i Soggetti Designati non possono raccogliere e conservare dati ulteriori rispetto a quelli strettamente necessari per l'esecuzione del mandato ricevuto.
Possono formare oggetto di trattamento i soli dati strettamente necessari all'esecuzione dell'incarico.
In presenza di dati trattati con strumenti elettronici i Soggetti Designati sono tenuti a:

- utilizzare le credenziali di autenticazione ricevute, composte da Username e Password, e a custodirle nel rispetto di quanto previsto dal Regolamento aziendale sulla sicurezza delle informazioni e sull'uso dei sistemi informatici.

In particolare, i Soggetti Designati devono:

- modificare le credenziali di autenticazione dopo il primo utilizzo ed ogni volta che dovessero sorgere dei dubbi sulla loro segretezza;
- non divulgarle a terzi;
- modificarle le credenziali almeno ogni 3 mesi;
- informare tempestivamente il proprio responsabile in caso di situazioni critiche dalle quali potrebbero verificarsi perdite o danneggiamenti dei dati trattati;
- impedire l'accesso non autorizzato ai dati provvedendo, nel caso di assenza anche momentanea dalla postazione di lavoro e a chiudere preventivamente tutte le applicazioni in uso sul proprio elaboratore.

In presenza di dati trattati anche senza l'ausilio di strumenti elettronici e di documenti cartacei, i Soggetti Designati sono tenuti a:
- verificare che i documenti utilizzati siano sempre sotto il proprio controllo e sotto la propria custodia per l'intero ciclo necessario allo svolgimento delle operazioni relative al trattamento dei dati, al fine di garantire che i documenti non siano visti o trattati da persone non autorizzate;
- riporre i documenti utilizzati, al termine del trattamento, nei relativi archivi e contenitori secondo le indicazioni ricevute dal proprio responsabile;
- effettuare le copie dei dati documenti cartacei solo se strettamente necessario ed in ogni caso trattarle con la stessa cura dei documenti originali, al termine del trattamento distruggere eventuali copie non utilizzate o comunque alterarle per impedirne la consultazione.

3.1 UTILIZZO DI SUPPORTI DI MEMORIZZAZIONE DEI DATI

Tutti i supporti magnetici rimovibili eventualmente forniti dalla società (dischetti, CD Rom, DVD, supporti USB, pen drive, hard disk, etc…) contenenti dati personali o informazioni di carattere lavorativo e/o

riservate devono essere trattati con particolare attenzione onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o recuperato successivamente alla cancellazione dai supporti. Tali supporti informatici devono essere conservati in luoghi sicuri al fine di evitare accessi non autorizzati e trattamenti non consentiti; in particolare, i supporti contenenti informazioni di carattere lavorativo e/o riservate e categorie particolari di dati personali e dati personali relativi a condanne penali e reati devono essere conservati in armadi/schedari/cassettiere che possano essere chiuse con chiave.

Occorre, altresì, cancellare dai dispositivi ad uso individuale eventuali dati personali, categorie particolari di dati personali, dati personali relativi a condanne penali e reati o di business che - per operazioni temporanee - fossero stati memorizzati sui dispositivi stessi.

I supporti informatici possono essere riutilizzati solo dopo aver provveduto a cancellare i dati e le informazioni in essi contenute; l'operazione deve essere compiuta in modo che i dati precedentemente memorizzati non siano tecnicamente ed in alcun modo recuperabili. Se l'operazione non è tecnicamente possibile, è necessario distruggere i supporti. Al fine di assicurare la distruzione e/o l'inutilizzabilità di supporti magnetici removibili, soprattutto se contenenti categorie particolari di dati personali, dati personali relativi a condanne penali e reati o informazioni di carattere lavorativo e/o riservate, ciascun utente dovrà informare il titolare del trattamento dei dati e, seguire le istruzioni da questi impartite.

I dati archiviati su supporti di tipo magnetico e/o ottico devono essere protetti con le stesse misure di sicurezza previste per i supporti cartacei.

E' vietato portare all'esterno dell'ambiente di lavoro supporti informatici contenenti dati personali, categorie particolari di dati personali, dati personali relativi a condanne penali e reati e/o informazioni di carattere lavorativo e/o riservate, se non necessario per lo svolgimento della

propria attività lavorativa e, senza la previa autorizzazione del Titolare del trattamento dei dati/Responsabile del trattamento dei dati.
E' vietato l'utilizzo di supporti rimovibili personali sugli strumenti aziendali.

3.2 PROTEZIONE ANTIVIRUS

Il sistema informatico aziendale e tutti i gli elaboratori elettronici sono protetti da eventuali attacchi virus mediante appositi programmi (software antivirus) aggiornati automaticamente. Nonostante ciò, ogni collaboratore deve, comunque, tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus, o mediate programmi maligni. Per ridurre la probabilità di tali attacchi è necessario che vengano osservate le seguenti regole:

- controllare che il programma antivirus sia installato correttamente, sia costantemente aggiornato e sia sempre attivo;
- non aprire file sospetti o dei quali si ha conoscenza di un comportamento sospetto;
- non introdurre applicazioni/software che non siano state preventivamente approvate o la cui provenienza sia dubbia;
- non utilizzare supporti magnetici di provenienza incerta;
- non utilizzare supporti magnetici già utilizzati su PC su cui è noto che si sono verificati malfunzionamenti;
- ogni supporto magnetico dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, prima dell'esecuzione dei file in esso contenuti; nel caso venga rilevato un virus, dovrà essere prontamente consegnato al titolare del trattamento dei dati;
- porre la massima attenzione sulle eventuali segnalazioni anomale inviate dal PC;

- usare correttamente e, solo per esigenze di lavoro, i servizi di posta elettronica e di Internet, evitando di aprire mail o relativi allegati sospetti, evitando di navigare su siti non professionali o non sicuri, evitando di scaricare file da Internet da siti non attendibili, etc.;
- non modificare le configurazioni impostate sul proprio PC.

Nel caso in cui il software antivirus rilevi la presenza di un virus, ciascun collaboratore è tenuto immediatamente a sospendere ogni elaborazione in corso, senza spegnere il computer e, segnalare prontamente l'accaduto al titolare del trattamento dei dati.

3.3 PROCEDURE PER LA RICHIESTA DI ASSISTENZA TECNICA, PER LE MODIFICHE ALLA CONFIGURAZIONE DEGLI ELABORATORI E PER LE VERIFICHE TECNICHE DA PARTE DEL PERSONALE ADDETTO

Il Titolare del trattamento rende noto che specifici tecnici informatici (interni o esterni all'azienda) sono autorizzati a compiere interventi nel sistema informatico aziendale diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware etc.). Tali tecnici hanno, inoltre, la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc. L'intervento potrà essere effettuato esclusivamente su richiesta dell'utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso. Pertanto, si evidenzia che per motivi di sicurezza

del sistema informatico, per motivi tecnici e/o manutentivi (aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc…), per finalità di monitoraggio e programmazione dei costi aziendali (ad esempio, verifica costi di connessione ad internet, traffico telefonico, etc...) e/o per finalità organizzative/produttive, sarà facoltà del Titolare del trattamento dei dati, tramite specifici tecnici informatici, interni e/o esterni alla azienda titolare del trattamento dei dati, di accedere, nel rispetto delle regole e delle procedure previste dalle vigenti normative, agli strumenti informatici aziendali e ai documenti ivi contenuti. Tali attività saranno, comunque, estranee a qualunque finalità di controllo dell'attività lavorativa. Per ogni necessità di assistenza nell'utilizzo delle risorse informatiche affidate a ciascun collaboratore e per richiedere ulteriori servizi o modifiche alla configurazione standard è necessario farne richiesta al titolare del trattamento dei dati.
Eventuali richieste che dovessero prevedere costi di hardware o licenze software dovranno essere preventivamente autorizzate dal Titolare del trattamento dei dati/Responsabile del trattamento dei dati.

3.4 CORRETTO UTILIZZO DELLA POSTA ELETTRONICA

E' obbligatorio porre la massima attenzione nell'aprire i file allegati alla posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti web o ftp non conosciuti o non ritenuti attendibili). Non aprire e-mail che contengono file allegati se non si conosce il mittente o il contenuto del file; in ogni caso mai aprire allegati con "particolari" estensioni (a titolo di esempio non esaustivo, .exe .bat .com .scr .pif); in caso di dubbio cancellare il messaggio senza aprire l'attachment. Non dare credito a messaggi che annunciano virus

pericolosissimi (Hoax virus), anche se inviati da mittenti apparentemente conosciuti; non rispedire tali messaggi ad altre persone e, in ogni caso, non modificare mai le impostazioni del proprio PC (es: cancellazione o spostamento di file o directory presenti sotto le cartelle c:\windows c:\winnt c:\programmi). I messaggi stile catena di S. Antonio che invitano a rispedire la mail ad altri indirizzi sono sempre falsi; le MAIL CHAIN sono proibite da Netiquette: è vietato rispedirle ed occorre cancellarle. Inoltre, si evidenzia di porre particolare attenzione in merito ad attacchi informatici che avvengono attraverso invio di mail contenenti il noto ramsonware c.d. "Cryptolocker". L'attacco del "Cryptolocker" avviene normalmente secondo questa modalità: l'ignaro utente riceve sulla propria casella di posta elettronica un messaggio che fornisce indicazioni ingannevoli su presunte spedizioni a suo favore oppure contenente un link o un allegato a nome di istituti di credito, aziende, enti, gestori e fornitori di servizi noti al pubblico. Il ramsonware si potrebbe trasmettere anche tramite e-mail che arrivano da contatti personali conosciuti, da mittenti già infettati dal virus. Cliccando sul link oppure aprendo l'allegato (in genere un documento in formato .pdf o .zip) si consente il download del ramsonware all'interno del proprio computer, che immediatamente inizierà a criptare il contenuto delle memorie all'interno del Pc e di quelle eventualmente collegate in rete. Così nel giro di poco tempo ci si troverà nell'impossibilità di accedere ai propri dati. A questo punto si realizza il ricatto dei criminali informatici che, per riaprire i file e rientrare in possesso dei propri documenti, richiedono agli utenti il pagamento di una somma di denaro a fronte della quale ricevere via e-mail un programma per la decriptazione. Per ridurre il rischio di cadere in tale truffa, è opportuno tenere sempre aggiornato il software del proprio computer, ma, soprattutto, fare attenzione a tutte le mail che si ricevono, soprattutto quelle non attese

e, in particolar modo, a non aprire gli allegati se sono in formati sconosciuti e con nomi che risultano "strani" per la loro grande lunghezza o perché privi di significato. Il rischio è legato al fatto che può capitare che il "CryptoLocker" non sia individuato dai sistemi di sicurezza informatica (antivirus, antispam, etc...) o lo sia solo dopo che la cifratura è iniziata o è stata completata, specie se una nuova versione sconosciuta a un antivirus viene distribuita. Una volta che ci si accorge di essere caduti nella trappola, l'unica possibilità è di resettare tutto il computer e ripristinarlo, utilizzando i back up salvati su memorie esterne. Ma, se si ha solo un sospetto di essere caduti in trappola, può essere importante scollegare immediatamente il Pc, spegnerlo, interrompendo l'alimentazione elettrica, perché questo inibirebbe il ramsonware dal propagarsi e, avvertire immediatamente il titolare del trattamento dei dati.

Più in generale, in caso di messaggi anomali o sospetti (es. mittenti sconosciuti, contenuto anomalo, etc…) vanno rispettate le seguenti regole:

- il messaggio non va aperto;
- nel caso in cui il messaggio si presenti al primo esame "normale" e solo dopo l'apertura sorga il sospetto, non va assolutamente aperto l'eventuale allegato (immagine, documenti, presentazioni, filmati, etc…) e/o non vanno cliccati i link presenti all'interno del messaggio stesso, in quanto eventuali infezioni possono propagarsi a seguito di queste azioni;
- l'e-mail va immediatamente cancellata.

3.5 CONSIGLI PRATICI PER CREARE UNA PASSWORD "FORTE"

Di seguito alcuni consigli pratici per creare una password "forte":

- Scegliere una combinazione casuale di lettere, numeri o simboli per creare una password esclusiva, che non sia associata alle

proprie informazioni personali (quali il proprio nome, il nome dei familiari, la data di nascita, animali domestici, il codice fiscale, etc…).

- Scegliere una password che appaia del tutto casuale agli altri e che, allo stesso tempo, si possa ricordare facilmente senza doverla scrivere.
- Creare una password di almeno 8 caratteri (più lunga è, più sicura sarà).
- All'atto del cambio periodico della password, ciascuna nuova password dovrà essere creata nella maniera più casuale possibile e dovrà risultare diversa dagli ultimi n. ... codici password utilizzati in precedenza.
- Non rivelare la propria password ad alcuno, per nessun motivo, anche se richiesta.
- La digitazione della password deve avvenire normalmente in maniera mascherata allo scopo di evitarne l'individuazione da parte di eventuali osservatori e comunque si raccomanda di evitare l'inserimento della propria password quando si è osservati.
- Non permettere ad altri utenti (es. colleghi) di operare con le proprie credenziali.
- Non scrivere mai la propria password, soprattutto non trascriverla su supporti (es. fogli, post-it, file, etc…) accessibili a terzi. Non lasciare note con la propria password sul computer o sulla scrivania (le persone che ci passano accanto possono facilmente rubare queste informazioni e utilizzarle). Nel caso sia assolutamente necessario conservarne traccia scritta, per propria memoria, essa deve essere conservata con cura ed in luogo sicuro, non accessibile a terzi;
- Non comunicare mai la password per telefono.

- Cambiare spesso la propria password (almeno con la frequenza prevista dalla normativa vigente, in base ai dati trattati).
- La password deve essere immediatamente sostituita, nel caso si sospetti che la stessa abbia perso la sua segretezza.
- La password deve essere sostituita con maggiore frequenza in occasione dello svolgimento di lavori particolarmente riservati.
- Ogni utente si impegna a notificare al Titolare del trattamento dei dati/Responsabile del trattamento dei dati l'avvenuto furto o smarrimento della password.

4. IL TRATTAMENTO INFORMATIZZATO DEI DATI

L'accesso alle banche dati, da parte delle risorse aziendali viene regolato attraverso un rigido protocollo di gestione delle credenziali di autenticazione ed autorizzazione.

All'Amministratore di Sistema è affidato il compito di gestire i privilegi informatici di accesso alle risorse aziendali utilizzando 5 tipologie di profili:

1) La Direzione e l'amministratore di sistema accedono con il profilo "admin": profilo che permette di visionare tutta la rete aziendale e fare modifiche alle cartelle di rete.

2) L'area Risorse Umane accede ai dati dei dipendenti e performances.

3) L'ufficio amministrativo accede esclusivamente ai dati necessari per la fatturazione.

4) I Team Leader hanno un profilo generico attraverso il quale accedono solo ai dati di performances per visionare l'andamento delle posizioni affidate.

5) Operatore/esattore: profilo che consente di accedere esclusivamente alle pratiche affidate, riservato agli operatori. Riconosce l'esistenza di eventuali pratiche collegate, ancora in lavorazione ma non può entrare nel dettaglio del fascicolo.

5. LA CONSERVAZIONE DEI DATI

L'Amministratore di Sistema ha il compito di vigilare affinché i sistemi informatici in uso presso la società rispettino le seguenti **modalità/tempistiche di conservazione dei dati** (il riferimento qui è sempre alle attività che Phonika S.p.A. pone in essere in qualità di Responsabile del trattamento per conto delle proprie Clienti/Committenti).

Alla conclusione delle attività di trattamento, l'accessibilità ai dati deve essere limitata al solo personale che potrebbe effettivamente necessitare di accedervi (ad es. direzione, amministrazione).

Al termine dell'affido da parte del cliente/committente, in ogni caso, i dati non devono più formare oggetto di trattamento per finalità di recupero crediti.

Phonika S.P.A. ha, in tal senso, applicato quanto previsto dal punto 4 del Provvedimento del Garante Privacy del 30 novembre 2005, "Liceità, correttezza e pertinenza nell'attività di recupero crediti": "*Salvo l'assolvimento di specifici obblighi di legge (ad esempio, per rendere conto delle attività svolte), che può richiedere una conservazione prolungata dei dati raccolti, una volta portato a termine l'incarico, i medesimi non devono formare oggetto di ulteriore trattamento. La loro eventuale conservazione ulteriore deve essere realizzata con modalità comunque tali da precluderne agli incaricati del trattamento la normale consultabilità (con l'adozione di opportune misure logiche o provvedendo alla trasposizione dei dati in archivi separati)*."

In relazione a tali circostanze sono adottate le seguenti modalità di conservazione dei dati raccolti.

Al termine dell'affido da parte del Cliente/Committente, i dati trattati durante la lavorazione devono essere separati (separazione logica) resi accessibili unicamente alla direzione e conservati per un periodo di dieci anni a decorrere dalla conclusione del mandato.

Tale termine corrisponde alle esigenze di conservazione imposte da specifiche norme di legge (ad es. normativa antiriciclaggio e adempimenti derivanti dalla licenza ex art. 115 TULPS) ed è parametrato al termine decennale della prescrizione dell'azione civile che potrebbe essere intentata contro la società.

Con riguardo alle procedure cd. di *call recording*, le registrazioni, laddove eseguite, sono archiviate per il tempo strettamente necessario - e comunque non superiore a 6 mesi - e conservate presso un data base ad uso esclusivo del personale facente parte delle funzioni Direzione, Risorse umane e Compliance.

Il periodo di conservazione di 6 mesi si rende necessario al fine di consentire il raggiungimento delle finalità di difesa, nonché poter esperire gli eventuali adempimenti di legge e rispondere alle contestazioni di terzi e/o richieste da parte dell'Autorità Giudiziaria.

Phonika S.p.A. provvede alla cancellazione dei dati oggetto di registrazione decorsi i 6 mesi dalla data di chiusura del periodo di affidamento, sempre che nel mentre non siano intervenute circostanze che, ai sensi di legge, ne impongano l'ulteriore conservazione.

Gli eventuali dati personali raccolti tramite la registrazione delle telefonate devono essere trattati esclusivamente dalle strutture aziendali interne e/o esternalizzate (in quest'ultimo caso nella forma di responsabile al trattamento dei dati) deputate alla gestione della infrastrutturazione tecnica, per finalità di difesa o per il miglioramento della qualità dei processi di recupero crediti, nel rispetto degli accordi sindacali vigenti.

5.1 DIPENDENTI, COLLABORATORI, CONSULENTI E FORNITORI.

Tempi di conservazione dei dati: i dati relativi ai rapporti di lavoro devono essere conservati per dieci anni. Tale termine è parametrato a quello decennale della prescrizione dell'azione civile che potrebbe essere intentata contro la società.

I dati acquisiti attraverso il sistema di call recording devono essere conservati per 6 mesi a decorrere dalla registrazione.

I dati acquisiti attraverso il sistema di videosorveglianza devono essere conservati per 48 ore (estendibili durante le festività del corrispondente periodo di chiusura dei locali aziendali). Il predetto termine è parametrato alle istruzioni provenienti in materia dall'Autorità di Controllo.

Adozione di misure tecniche ed organizzative per la conservazione dei dati: alla conclusione del rapporto di lavoro, i dati devono essere separati e protetti attraverso l'applicazione di misure tecniche ed organizzative ulteriori rispetto a quelle adottate per il trattamento dei dati di uso corrente. Alla conclusione del periodo di conservazione deve essere prevista una specifica procedura di cancellazione dei dati.

5.2 CLIENTI PHONIKA S.P.A.

Tempi di conservazione dei dati: i dati relativi all'esecuzione degli impegni contrattualmente assunti sono conservati per un periodo di dieci anni, a decorrere dalla conclusione del contratto. Tale termine è parametrato a quello decennale della prescrizione dell'azione civile che potrebbe essere intentata contro la società.

Adozione di misure tecniche ed organizzative per la conservazione dei dati: alla conclusione del rapporto contrattuale, i dati vengono separati e protetti attraverso l'applicazione di misure tecniche ed organizzative ulteriori rispetto a quelle adottate per il trattamento dei dati di uso corrente. Alla conclusione del periodo di conservazione è prevista una specifica procedura di cancellazione dei dati.

Il presente documento è stato redatto con la collaborazione del Responsabile della Protezione dei Dati.