Livenza Servizi Mobilità S.r.l.

REGOLAMENTO INTERNO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

ISTRUZIONI PER L'USO DEGLI STRUMENTI FORNITI (ELETTRONICI E NON), e ISTRUZIONI OPERATIVE PER SOGGETTI AUTORIZZATI AL TRATTAMENTO

INDICE

1. FINALITÀ DEL REGOLAMENTO

La finalità del presente documento è quella di descrivere i principi generali di sicurezza e gli obblighi di riservatezza delle informazioni e dei dati personali, che il titolare del trattamento garantisce ed assicura a tutti i soggetti coinvolti nell'ambito del trattamento dei dati, con l'intento di sviluppare un efficiente sistema di gestione delle procedure e dei processi per la sicurezza dei dati nel rispetto dei diritti e delle libertà fondamentali nonché della dignità delle persone fisiche, in ottemperanza al Regolamento UE n. 2016/679 (di seguito, "GDPR").
In particolare, il presente Regolamento vuole costituire uno strumento fondamentale per potenziare nei soggetti adibiti al trattamento dei dati all'interno della struttura l'analisi e la consapevolezza dei rischi e delle insidie che possono coinvolgere la gestione e l'utilizzo dei sistemi informativi automatizzati, oltre all'archivio cartaceo, al fine di prevenire e ridurre situazioni di pericolo, quali la perdita dei dati, l'accesso non autorizzato o il trattamento non consentito o non conforme.

2. AMBITO DI APPLICAZIONE

Il presente Regolamento si applica a tutte le persone fisiche che, nell'esercizio delle proprie mansioni e nell'ambito delle rispettive competenze, svolgono attività in qualità di "*incaricato/autorizzato del trattamento dei dati personali*" ai sensi dell'art. 28 del GDPR (personale dipendente, collaboratori, stagisti, ecc.), nonché ai soggetti, incluse le persone giuridiche, che, in qualità di "*Responsabili esterni del trattamento*", collaborano alla gestione delle informazioni e trattano, per conto del titolare del trattamento, dati personali di titolarità della Società.
Con riferimento all'ambito oggettivo, il Regolamento si applica alle diverse attività che comportano il trattamento dei dati personali di titolarità della Società (quali, ad esempio, attività connesse alla gestione del personale, adempimenti relativi ai rapporti contrattuali con i fornitori, ecc.), come puntualmente specificate all'interno del "Registro delle attività di trattamento" predisposto dal Titolare ai sensi dell'art. 30, paragrafo primo, del GDPR. I dipendenti, i collaboratori, i consulenti ed in generale tutte le persone autorizzate ad accedere ai dati personali e preposte allo svolgimento delle operazioni di trattamento relative ai dati, devono ispirarsi a un principio generale di diligenza e correttezza.
Ogni utilizzo dei dati in possesso della Società diverso da finalità strettamente professionali, è espressamente vietato.

3. DEFINIZIONI

Come stabilito dall'articolo n. 4 del Regolamento Europeo n. 2016/679, ai fini di questo disciplinare si intende per:

a) «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può esser 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;
b) «titolare»: persona fisica, persona giuridica, pubblica amministrazione e qualsiasi altro ente, associazione o organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.
c) «responsabile»: persona fisica, persona giuridica, pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal Titolare al trattamento di dati personali. Individuati tra coloro che per esperienza, capacità ed affidabilità sono in grado di fornire idonea garanzia del pieno rispetto delle indicazioni del presente Regolamento e della normativa vigente.

d) «incaricati/autorizzati»: persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal Responsabile.
e) «interessato»: persona fisica cui si riferiscono i dati personali
f) «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;
g) «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
h) «profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
i) «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;
j) «archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
k) «destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
l) «terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
m) «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;
n) «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;
o) «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;
p) «dati biometrici»: i 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;

q) «**dati relativi alla salute**»: i 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;

r) «**autorità di controllo**»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del Regolamento UE;

Quelle sopra riportate, di cui si è data evidenza, rappresentano le "definizioni" su cui ha inciso maggiormente il nuovo Regolamento europeo: per le altre "definizioni" si fa espresso rinvio al testo dell'articolo n. 4 del Regolamento Europeo n. 2016/679.

4. PRINCIPI APPLICABILI AL TRATTAMENTO DEI DATI

Nella pianificazione o nell'espletamento di qualsiasi attività, la Società si impegna a garantire e a dimostrare che il trattamento dei dati avvenga in maniera conforme a quanto previsto dalla normativa italiana ed europea in materia di protezione dei dati e, in particolare, nel puntuale rispetto dei fondamentali principi enunciati all'art. 5 del GDPR:

- **Liceità**. Un trattamento è lecito solo se fondato su uno dei presupposti individuati dalla normativa. Per ogni trattamento effettuato all'interno della struttura della Società è puntualmente individuata, all'interno del Registro delle attività di trattamenti *ex* art. 30 del GDPR, una specifica base giuridica. Inoltre, all'interno delle informative *ex* 8 art. 13-14 fornite agli interessati viene esplicitata la base giuridica inerente i dati raccolti.
- **Trasparenza e correttezza**. Sono comunicate in maniera esplicita ai soggetti interessati le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati i dati personali nonché la misura in cui tali dati sono o saranno trattati; inoltre le comunicazioni relative al trattamento dei dati personali sono, come richiesto dalla normativa, facilmente accessibili e comprensibili tramite l'utilizzo di un linguaggio semplice e chiaro.
- **Limitazione della finalità**. I dati devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non vi sia incompatibilità con tali finalità. Al fine di rispettare tale principio, il titolare del trattamento aggiornerà i moduli di informativa in conseguenza di eventuali modifiche al Registro delle attività di trattamento *ex* art. 30 del GDPR, nonché fornirà all'interessato il modulo dell'informativa aggiornato nel caso in cui dovesse utilizzare i dati personali per finalità diverse da quelle per cui essi sono stati raccolti.
- **Minimizzazione dei dati**. I dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati. Al fine di rispettare tale principio la Società definisce ed implementa misure tecniche e organizzative adeguate al fine di garantire che siano trattati solo i dati personali necessari per ogni specifica finalità del trattamento.
- **Esattezza**. I dati devono essere esatti e, se necessario, aggiornati; in tal senso la Società ha previsto, al suo interno, procedure operative ed organizzative al fine di poter garantire tempestivamente il riscontro alle richieste degli interessati in relazione all'accesso, alla modifica o alla rettifica dei dati personali trattati. Tali diritti vengono indicati, in maniera esplicita e con chiarezza, nelle informative fornite agli interessati.
- **Limitazione della 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. La Società, con la consulenza del DPO, al fine di ottemperare ai principi inerenti la conservazione, prevede un adeguato processo finalizzato ad indicare, per ogni trattamento, le politiche di conservazione e gli interventi mirati per procedere alla corretta identificazione dell'interessato, alla cancellazione o all'anonimizzazione di tali dati. Gli interessati

hanno il diritto di richiedere che i propri dati personali siano cancellati e non più sottoposti a trattamento qualora la conservazione di tali dati violi le norme previste.

- Integrità e riservatezza. I dati devono essere trattati in maniera da garantirne un'adeguata sicurezza, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti (accesso o utilizzo non autorizzato) e dalla perdita, dalla distruzione o dal danno anche solo accidentali. A tal proposito l'Ente garantisce che i dati non siano comunicati a soggetti che non abbiano la necessità lavorativa di venirne a conoscenza, secondo la regola in base alla quale ogni incaricato o soggetto autorizzato al trattamento può trattare solo i dati personali di competenza, necessari per il conseguimento delle rispettive finalità. Il rispetto dei suddetti principi nonché la garanzia di protezione e di adozione di corrette misure di sicurezza è, inoltre, richiesta ai soggetti terzi che, in qualità di responsabili esterni, hanno assunto l'incarico della gestione di alcuni trattamenti per conto del Titolare.

5. LA POLITICA DI SICUREZZA INTERNA. ADEMPIMENTI E REGOLE DI CONDOTTA

Sulla scorta dei principi enunciati sopra, la Società assicura che il trattamento dei dati personali avvenga con modalità tali da preservarne l'integrità e la confidenzialità mediante l'adozione di misure di sicurezza, anche preventive, idonee ad evitare situazioni di rischio e di non conformità o di alterazione dei dati. Al riguardo la Società, in veste di Titolare del trattamento, è tenuta ad effettuare, nei confronti di tutti i soggetti che trattano dati, verifiche e controlli sulla correttezza del trattamento assegnato. In particolare, ciascun autorizzato al trattamento deve:

- rispettare i principi generali del Regolamento UE 2016/679 (GDPR), con particolare riferimento alla liceità e correttezza del proprio agire, all'obbligo di procedere alla raccolta e alla registrazione dei dati per scopi determinati, espliciti e legittimi;
- rispettare l'obbligo di riservatezza e segretezza e conseguentemente il divieto di comunicazione e diffusione dei dati trattati nel corso dell'incarico svolto;
- utilizzare i dati, cui abbia accesso, solamente per finalità compatibili all'esecuzione delle proprie mansioni o dei compiti affidati, per i quali si è autorizzati ad accedere alle informazioni e ad utilizzare gli strumenti della Società;
- eseguire qualsiasi altra operazione di trattamento nei limiti delle proprie mansioni e nel rispetto delle norme di legge;
- rispettare le misure di sicurezza idonee adottate dalla Società, atte a salvaguardare la riservatezza e l'integrità dei dati;
- segnalare eventuali malfunzionamenti di strumenti elettronici, perdite di dati o esigenze (sia di natura organizzativa, sia tecnica), che possano migliorare lo svolgimento delle operazioni affidate;
- in caso di interruzione del lavoro, anche temporanea, verificare che i dati trattati non siano accessibili a terzi non autorizzati;
- mantenere riservate le proprie credenziali di autenticazione;
- svolgere le attività previste dai trattamenti secondo le direttive del titolare o, se nominato, responsabile interno del trattamento dei dati;
- non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del titolare o, se nominato, del responsabile interno del trattamento dei dati;
- rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali;
- informare il titolare o, se nominato, il responsabile interno in caso di incidente di sicurezza che coinvolga dati particolari e non;

- raccogliere, registrare e conservare i dati presenti negli atti e documenti contenuti nei fascicoli e nei supporti informatici avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;
- seguire i corsi di formazione in materia di disciplina della protezione dei dati, secondo le indicazioni e modalità fornite dal titolare.

6. ISTRUZIONI OPERATIVE PER IL TRATTAMENTO DEI DATI DA PARTE DEI SOGGETTI AUTORIZZATI

I dipendenti, i collaboratori e, in generale, tutte le persone autorizzate ad accedere ai dati personali e preposte allo svolgimento delle operazioni di trattamento relative ai dati, devono ispirarsi ai principi generali di diligenza e correttezza. L'utilizzo dei dati personali deve avvenire in base al fondamentale principio del "*need to know*", secondo cui questi non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative (anche se queste persone sono a loro volta incaricate del trattamento). Ogni utilizzo dei dati in possesso della Società diverso da finalità strettamente professionali è espressamente vietato.

Di seguito vengono esposte le principali istruzioni operative e le regole comportamentali che ogni "incaricato" deve seguire per evitare e prevenire condotte che, anche inconsapevolmente o incolpevolmente, potrebbero comportare rischi alla sicurezza del patrimonio informativo e all'immagine della Società.

6.1. MODALITÀ DI SVOLGIMENTO DELLE OPERAZIONI

Le principali operazioni degli autorizzati del trattamento sono:

- identificazione dell'interessato: al momento della raccolta dei dati personali, qualora sia necessario individuare l'identità del soggetto che fornisce le informazioni, è obbligatorio richiedere un documento di identità o di riconoscimento, al fine di verificare la identità e di procedere correttamente alla raccolta e alla registrazione delle informazioni;
- verifica del controllo dell'esattezza del dato e della corretta digitazione: al momento della registrazione dei dati raccolti, occorre prestare attenzione alla digitazione e all'inserimento dei dati identificativi e degli altri dati riferiti all'interessato, al fine di evitare errori, che potrebbero generare problemi nella corretta gestione dell'anagrafica e nello svolgimento delle operazioni, che caratterizzano il processo di trattamento;
- norme logistiche per l'accesso fisico ai locali: i locali, ove sono custoditi i dati personali (ed in particolare quelli di natura sensibile), devono essere soggetti a controllo e a verifica, al fine di evitare che durante l'orario di lavoro possano essere conosciuti o accessibili da parte di soggetti non autorizzati. Si raccomanda, in caso di allontanamento dal proprio ufficio o dalla propria postazione di lavoro, di adottare tutte le accortezze e precauzioni al fine di impedire l'accesso fisico a chi non sia legittimato, soprattutto se esterno all'organizzazione di appartenenza. Laddove si esegue un trattamento di dati personali, deve essere possibile ricoverare in luogo sicuro i documenti cartacei e i supporti rimovibili contenenti tali dati. Pertanto le porte degli uffici ed almeno un armadio per ufficio devono essere dotati di serratura con chiave. Al termine dell'orario lavorativo, ove la dinamica delle attività ed il numero di occupanti lo consentano, è necessario chiudere sempre a chiave gli uffici nei quali vengono svolti trattamenti di dati personali o gli armadi o cassetti ove sono contenuti i documenti;
- rilevazione presenze: ove possibile, si raccomanda di dotare la/le sede/i della Società di un servizio di rilevazione delle presenze e di un servizio di reception / sorveglianza. In questo caso, ogni soggetto autorizzato è tenuto ad utilizzare sempre i sistemi di rilevazione presenze disponibili, allo

scopo di segnalare la propria presenza e legittimare le attività in corso di svolgimento.

6.2. ISTRUZIONI PER L'USO DEGLI STRUMENTI INFORMATICI

Come principio generale, sia i dispositivi di memorizzazione del proprio PC sia le unità di rete, devono contenere informazioni strettamente professionali e non possono essere utilizzate per scopi diversi (immagini, video e documenti personali).
Di seguito sono riportate le indicazioni per la gestione dei diversi strumenti informatici per il trattamento dati:

a) Gestione strumenti elettronici (PC fissi e portatili)

Ciascun autorizzato è responsabile del corretto utilizzo e della custodia degli strumenti elettronici in dotazione (a titolo esemplificativo personal computer, periferiche, lettori di smart card).
Si devono adottare le misure di sicurezza per la tutela della riservatezza, consistenti nell'evitare che l'accesso ai dati possa avvenire da parte di soggetti estranei all'organizzazione o non specificamente autorizzati.
Per la gestione della sessione di lavoro sul PC (fisso e portatile), è necessario osservare quanto segue:

- al termine delle ore di servizio, il PC deve essere spento, a meno che non stia svolgendo elaborazioni particolari. In tal caso gli uffici debbono tassativamente essere chiusi a chiave;
- se il soggetto autorizzato si assenta momentaneamente dalla propria postazione deve accertarsi che l'eventuale sessione di lavoro aperta non sia accessibile da altre persone. Pertanto deve chiudere la sessione di lavoro sul PC facendo Logout, oppure in alternativa deve avere attivo un salvaschermo (screen- saver) protetto dalle credenziali di autenticazione.

Relativamente all'utilizzo dello screen-saver, occorre osservare le seguenti norme:

- Non deve mai essere disattivato;
- Il suo avvio automatico deve essere previsto non oltre i primi 10 minuti di inattività del PC;
- Deve essere messo in funzione manualmente ogni volta che si lascia il PC incustodito ed acceso.

Quando si esegue la stampa di un documento contenente dati personali occorre:

- ritirare tempestivamente i documenti stampati per evitare l'accesso a soggetti non abilitati al trattamento;
- non abbandonare presso il fotocopiatore e la stampante documenti leggibili;
- maneggiare e custodire con cura le stampe di materiale riservato;
- non lasciare accedere alle stampe persone non autorizzate;
- se la stampante non si trova nelle vicinanze della scrivania, recarsi il più in fretta possibile a ritirare le stampe;
- per stampe riservate, cercare di utilizzare una stampante non condivisa oppure la modalità di stampa ritardata impostando un tempo sufficiente a permettere il raggiungimento del dispositivo prima dell'inizio della stampa;
- distruggere personalmente le stampe quando non più necessarie, oppure in caso di "brutte copie"/bozze da ristampare perché errate;
- prestare attenzione alle fotocopie: fare fotocopie di documenti contenenti dati personali sensibili solo se strettamente necessario. Assicurarsi di non lasciare copie all'interno del dispositivo e, se necessario, per eliminare copie mal riuscite utilizzare una macchina distruggi-documenti (ove presente).
- non gettare nel cestino le stampe di documenti che possono contenere informazioni confidenziali.

Per l'utilizzo dei PC portatili valgono le regole elencate per i PC connessi alla rete, con le seguenti ulteriori raccomandazioni:

- prima della riconsegna, rimuovere eventuali file ivi elaborati;
- quando il PC portatile è nei locali della Società, non lasciarlo mai incustodito; in caso di brevi assenze assicurarlo alla scrivania o ad elementi "sicuri" dell'arredamento (maniglie, intelaiature…) utilizzando gli appositi cavi in acciaio dotati di lucchetto;
- quando il PC portatile è all'esterno della Società, evitare di lasciarlo incustodito;
- per assenze prolungate, anche qualora l'ambiente venga ritenuto "affidabile", è necessario custodire il portatile in modo opportuno;
- in caso di furto di un portatile è necessario avvertire tempestivamente il responsabile del Servizio Informatico, onde prevenire possibili intrusioni ai sistemi interni della Società;
- in caso di viaggio aereo trasportare tassativamente il portatile come bagaglio a mano;
- eseguire periodicamente salvataggi dei dati e non tenere tali backup insieme al PC portatile.

b) Gestione username e password

L'accesso al PC, sia esso collegato in rete o meno, è protetto da un sistema di autenticazione che richiede all'autorizzato di inserire sulla videata di accesso all'elaboratore un codice utente (USERNAME) ed una parola chiave (PASSWORD).
L'adozione ed il corretto utilizzo della combinazione username / password è fondamentale per il corretto utilizzo del PC, in quanto:

- tutela l'utilizzatore ed in generale la Società da accessi illeciti, atti di vandalismo e, in generale, violazioni e danneggiamenti del proprio patrimonio informativo;
- tutela il soggetto autorizzato da false imputazioni, garantendo che nessuno possa operare a suo nome e che, con il suo profilo (ossia con le sue user id e password) solo lui possa svolgere determinate azioni;
- è necessario per gestire correttamente gli accessi a risorse condivise.

Ciascun autorizzato deve scegliere le password in base ai seguenti criteri:

- devono essere lunghe almeno otto caratteri;
- non devono fare riferimento ad informazioni agevolmente riconducibili ai soggetti utilizzatori o ai loro famigliari;
- devono contenere una combinazione di numeri e/o segni speciali, lettere, maiuscole e minuscole;
- non deve essere uguali alle precedenti;
- non deve contenere più di due caratteri consecutivi identici (es: aaaaa…);
- non deve contenere sequenze di cifre consecutive (es: 12345…);
- non deve essere basata su parole di uso comune (nomi di luoghi, personaggi, mesi, giorni della settimana, ecc.).

Per la corretta gestione della password è necessario osservare le seguenti norme:

- almeno ogni 3 mesi, in caso di dati sensibili, o 6 in caso di dati comuni, è obbligatorio cambiare la password;
- ogni password ricevuta va modificata al primo utilizzo;
- la password venga conservata in un luogo sicuro;
- non rivelare o condividere la password con i colleghi di lavoro, famigliari e amici, soprattutto attraverso il telefono;
- non utilizzare la funzione, offerta da alcuni software, di salvare automaticamente la password per

successivi utilizzi delle applicazioni.

c) Installazione di hardware e software

L'installazione di hardware e software, nonché la modifica dei parametri di configurazione, possono essere eseguiti solamente dalle persone del Servizio Informatico su mandato del Responsabile del trattamento per i Sistemi Elettronici, se nominato, o del Titolare. Pertanto si raccomanda agli utenti dei PC di rispettare i seguenti divieti:

- non utilizzare sul PC dispositivi personali, o comunque non interni della Società, quali lettori dispositivi di memorizzazione dei dati;
- non installare sistemi per connessione esterne (es: modem, wifi); tali connessioni, aggirando i sistemi preposti alla sicurezza della rete interna della Società, aumentano sensibilmente i rischi di intrusioni e di attacchi dall'esterno;
- non installare programmi, anche in versione demo. In particolare, è vietata l'installazione di giochi, programmi in prova (shareware), programmi gratuiti (freeware), programmi pirata, e in generale tutti i software non autorizzati dal Servizio Informatico;
- non modificare i parametri di configurazione del proprio PC senza espressa autorizzazione e senza il supporto di personale tecnico qualificato.

Si ricorda che normalmente la condivisione di aree e di risorse del proprio PC è vietata. Può essere autorizzata dal Servizio Informatico, solo in casi eccezionali e solo per il tempo strettamente necessario allo svolgimento delle attività di lavoro. In questi casi devono essere adottate password di lettura e scrittura e la condivisione deve operare solo su singole directory del PC, e non sull'intero disco rigido.

d) Gestione posta elettronica interna

Il servizio di posta elettronica viene fornito per permettere la comunicazione con soggetti terzi interni ed esterni per le finalità della Società e in stretta connessione con l'effettiva attività e mansioni del lavoratore o del volontario che utilizza tale funzionalità.
Al fine di non compromettere la sicurezza della Società e di prevenire conseguenze legali a carico della stessa, bisogna adottare le seguenti norme comportamentali:

- se si ricevono mail da destinatari sconosciuti contenenti file di qualsiasi tipo, procedere alla loro immediata eliminazione.
- è fatto divieto di utilizzare le caselle di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail list, salvo diversa ed esplicita autorizzazione.
- la casella di posta elettronica assegnata deve essere mantenuta in ordine, cancellando i documenti inutili specialmente se contengono allegati ingombranti come dimensione.

Nell'ipotesi in cui la email debba essere utilizzata per la trasmissione di dati particolari (ex dati sensibili), si raccomanda di prestare attenzione a che:

- l'indirizzo del destinatario sia stato correttamente digitato,
- l'oggetto del messaggio non contenga direttamente il riferimento a stati, fatti o qualità idonei a rivelare dati di natura sensibile;
- nel corpo del messaggio sia presente un'intestazione standardizzata in cui si avverta della confidenzialità/riservatezza del messaggio;
- ove possibile criptare o cifrare la mail.

Si ricorda che la corrispondenza relativa agli indirizzi di posta elettronica generici, condivisi tra più lavoratori (es.: info@ente.it; urp@ente.it; ufficioreclami@ente.it), ha natura non privata.

Invece, nel caso di indirizzo di posta elettronica personale, messo a disposizione dalla Società, il lavoratore potrà – per i casi di assenza prolungata e di improrogabili necessità legate all'attività lavorativa – inserire dei messaggi di risposta automatica con le coordinate di altri lavoratori cui rivolgersi o delegare un altro lavoratore (fiduciario) a verificare il contenuto dei messaggi a lui indirizzati e a inoltrare al titolare quelli ritenuti rilevanti per l´ufficio.

e) Gestione del salvataggio dei dati

- per i dati ed i documenti che risiedono sui server gestiti centralmente, come ad esempio cartelle di rete e database, il Servizio Informatico esegue i salvataggi con la possibilità di ripristinare in toto oppure selettivamente eventuali files distrutti, ad esempio per guasti hardware oppure per cancellazioni involontarie.
- per i dati ed i documenti che risiedono esclusivamente sul PC, ogni soggetto autorizzato deve eseguire almeno una volta alla settimana la copia (salvataggio, o backup). Questo allo scopo di garantire la disponibilità ed il ripristino dei dati personali nel caso di una generica compromissione delle risorse (cancellazioni accidentali, guasti, furti…). Il soggetto autorizzato deve verificare che i supporti informatici utilizzati per il backup, che normalmente sono dischi esterni, CD, DVD oppure flash disks (chiavette) siano funzionali e non corrotti.

f) Gestione dei supporti rimovibili

I supporti rimovibili, come ad esempio dischi magnetici esterni, penne USB o CD riscrivibili, quando contengono dati personali devono essere custoditi in luogo protetto e non accessibile (cassaforte, armadio chiuso a chiave, etc.). Quando non sono più utilizzati devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri Incaricati non autorizzati al trattamento degli stessi dati, soltanto dopo essere stati formattati.
Il trasferimento di file contenenti dati personali, dati particolari (ex dati sensibili) e giudiziari su supporti rimovibili, è da eseguire unicamente in via transitoria, ponendo la massima attenzione alla destinazione di trasferimento e cancellando i file appena possibile.
I dati particolari (ex dati sensibili)/giudiziari devono essere crittografati.

g) Gestione protezione dai virus informatici

Per prevenire eventuali danneggiamenti al software causati dalla presenza o dall'azione di programmi virus informatici, su ogni elaboratore della Società è stato installato un software antivirus che si aggiorna all'ultima versione disponibile.
L'antivirus della Società non deve mai essere disattivato o sostituito con altro antivirus non ufficialmente fornito.
Nel caso il programma antivirus installato sul proprio PC riscontri la presenza di un virus, oppure si sospetti la presenza di un virus non rilevato dal programma antivirus è necessario darne immediatamente segnalazione al responsabile del Servizio Informatico o al Titolare.
Si raccomanda di non scaricare e né tantomeno aprire file provenienti via e-mail da mittenti sconosciuti. Tali file, possono essere portatori di virus e compromettere la funzionalità del PC, l'integrità dei dati in esso contenuti e soprattutto l'integrità dei sistemi collegati al PC stesso.

6.3. ISTRUZIONI PER L'USO DEGLI STRUMENTI "NON ELETTRONICI"

a) Modalità di trattamento

Per i trattamenti di dati personali effettuati senza l'ausilio di strumenti elettronici (sia i documenti

cartacei sia documenti di altro tipo come ad esempio microfilm, microfiche e lucidi), l'incaricato è tenuto ad osservare le seguenti disposizioni ed istruzioni:

- i documenti contenenti dati personali non devono essere portati al di fuori dei locali individuati per la loro conservazione se non in casi del tutto eccezionali, e, qualora ciò avvenga, l'asportazione deve essere ridotta al tempo minimo necessario per effettuare le operazioni di trattamento. Per tutto il periodo in cui i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici sono al di fuori dei locali individuati per la loro conservazione, l'incaricato del trattamento non dovrà lasciarli mai incustoditi; è vietato il deposito di documenti di qualsiasi genere negli ambienti di transito o accessibili da soggetti terzi (corridoi o sale). Nel caso dei dati "particolari" (dati sensibili), il rispetto di queste norme è essenziale.
- verificare che i documenti cartacei contenenti dati personali, composti da numerose pagine o più raccoglitori, siano sempre completi ed integri. Al termine dell'orario di lavoro l'incaricato del trattamento deve riportare tutti i documenti nei locali individuati per la loro conservazione.
- i documenti contenenti dati personali non devono essere mai lasciati incustoditi o abbandonati (su tavoli, scrivanie) durante l'orario di lavoro, quando ci si debba assentare dal proprio posto (ad esempio per la pausa pranzo o per una riunione): è infatti necessario identificare un luogo sicuro di custodia che dia sufficienti garanzie di protezione da accessi non autorizzati (un armadio o un cassetto chiusi a chiave, ecc.).
- al momento della consegna di copie dei documenti ai destinatari è necessario adottare tutte le garanzie di sicurezza, quali l'utilizzo di buste sigillate (in particolare in presenza di dati di natura sensibile).
- adozione di ogni opportuna cautela affinché persone non autorizzate non vengano a conoscenza del contenuto dei suddetti documenti.
- per evitare il rischio di diffusione o comunicazione non autorizzata dei dati personali trattati senza l'ausilio di strumenti elettronici, si deve limitare l'utilizzo di copie fotostatiche; il numero di copie di documenti contenenti dati personali deve essere strettamente funzionale alle esigenze di lavoro; particolare cautela deve, inoltre, essere adottata quando i documenti sono consegnati in originale ad un altro incaricato debitamente autorizzato.
- è vietato utilizzare copie fotostatiche di documenti contenenti dati personali, e in particolare dati sensibili, come carta da riciclo o da appunti.
- i documenti contenenti dati "sensibili" (ad esempio i dati riguardanti lo stato di salute o i dati sanitari) o dati che, per una qualunque ragione, siano stati indicati come meritevoli di particolare attenzione, devono essere custoditi con molta cura o in contenitori ed appositi armadi muniti di serratura, ove previsto.
- l'accesso ai supporti deve essere limitato al tempo necessario a svolgere i trattamenti previsti;
- i supporti devono essere archiviati in ambiente ad accesso controllato;
- la documentazione contenente dati personali che, per ragioni di praticità operativa, risiede sulle scrivanie degli autorizzati, deve comunque essere rimossa al termine dell'orario di lavoro;

L'autorizzato deve attenersi alle seguenti prescrizioni:

- quando gli atti e i documenti contenenti dati personali, dati particolari (ex dati sensibili) o giudiziari sono affidati agli incaricati per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate;
- l'accesso agli archivi contenenti dati particolari (ex dati sensibili) o giudiziari deve essere

controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono devono essere preventivamente autorizzate.

Infine, a seguito di una cessazione del rapporto lavorativo o di consulenza o, comunque, al venir meno, ad insindacabile giudizio della Società, della permanenza dei presupposti per l'utilizzo dei dati cartacei, gli incaricati hanno i seguenti obblighi:

- procedere immediatamente alla restituzione dei dati cartacei in loro possesso;
- divieto assoluto di copiare, alterare, manomettere o distruggere i dati cartacei assegnati o renderli inintelligibili, tramite qualsiasi processo.

b) Distruzione delle copie cartacee

Coloro che sono preposti alla duplicazione di documentazione (con stampanti o fotocopiatrici o altre periferiche) ovvero che utilizzando strumenti per la riproduzione cartacea di documenti digitali, sono tenuti a procedere alla relativa distruzione del supporto, qualora si verifichino errori o la riproduzione non sia corretta, evitando di riutilizzare i fogli, salva l'ipotesi di uso esclusivamente personale per eventuali appunti o brutte copie, da distruggere immediatamente quando non più necessarie.
La distruzione di documenti contenenti dati personali deve essere operata, ove possibile, direttamente dal personale autorizzato.

c) Misure di sicurezza

Il trattamento sicuro di documenti contenenti dati personali richiede la presenza di misure di sicurezza con le quali il soggetto autorizzato possa interagire ed una serie di accorgimenti direttamente gestibili dal soggetto autorizzato stesso. In particolare, si richiede:

- la presenza e l'uso tassativo di armadi e/o cassetti dotati di serratura adeguata;
- la presenza e l'uso tassativo, ove si richieda la distruzione di documenti contenenti dati particolari (ex dati sensibili) e giudiziari, di un tritadocumenti. Ove non siano disponibili strumenti per la distruzione dei documenti (trita documenti), o il volume di questi sia tale da imporre il ricorso al servizio di macero, il personale autorizzato che avvia al macero la documentazione è tenuto a confezionare tale documentazione in modo che il pacco risulti anonimo e solido.

7. ADDETTI ALLA MANUTENZIONE

Le seguenti istruzioni devono essere osservate dai preposti in qualità di addetti alla gestione o manutenzione che trattano dati di titolarità per i quali è nominato un responsabile del trattamento nonché dagli addetti di ditte specializzate che svolgano interventi tecnici di gestione e manutenzione degli strumenti elettronici:

- effettuare operazioni di manutenzione e supporto per verifica corretto funzionamento (monitoraggio e diagnostica) su flussi dei dati;
- gestire le credenziali di autenticazione dei soggetti incaricati del trattamento su indicazione dell'Amministratore di sistema;
- gestire i profili di autorizzazione degli incaricati al trattamento dei dati, su specifiche impartite dai responsabili di funzione/BU, su indicazione dell'Amministratore di sistema;
- provvedere alla disattivazione/variazione delle utenze, ivi compreso l'account di posta elettronica, assegnate al personale cessato dal servizio o che abbia modificato il proprio ambito di trattamento, su richiesta specifica dei responsabili ovvero della Direzione Risorse Umane e su indicazione

dell'Amministratore di sistema;
- ❖ custodire la documentazione cartacea, prodotta nello svolgimento dei propri compiti istituzionali.

L'accesso agli addetti alla gestione e manutenzione è consentito unicamente ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere alle operazioni di manutenzione dei programmi o del sistema informatico.
A ciascun addetto alla manutenzione, previa sottoscrizione di apposito atto per accettazione, è pertanto consentito eseguire le operazioni strettamente necessarie a tali scopi e/o richieste dal titolare, secondo le seguenti istruzioni operative:

- ❖ nel caso in cui sia necessario effettuare stampe di prova per controllare il funzionamento di stampanti o per verificare il funzionamento di strumenti o programmi installati, non utilizzare files già esistenti ma creare files di prova.
- ❖ nel caso si renda strettamente necessario accedere a files contenenti dati (ad esempio per il recupero di un testo) limitare l'accesso ai dati per il tempo strettamente necessario all'assolvimento delle operazioni di manutenzione.
- ❖ per effettuare operazioni di manutenzione sui database della Società che prevedano la raccolta e la conservazione dei dati, tali dati dovranno essere custoditi in modo tale da non essere accessibili da soggetti non autorizzati.
- ❖ devono inoltre essere adottate le misure di sicurezza minime previste dal codice in materia di protezione dei dati personali.
- ❖ è necessario informare al più presto il titolare o il responsabile del trattamento qualora si dovessero riscontrare malfunzionamenti o non conformità.
- ❖ tutti i dati personali contenuti nei data base devono essere protetti da password.
- ❖ nel caso in cui sia necessario accedere ai dati attraverso gli strumenti elettronici in dotazione agli incaricati, attenersi alle seguenti indicazioni:
  - in presenza dell'autorizzato, far digitare la password dall'autorizzato stesso evitando di venirne a conoscenza;
  - o in assenza dell'autorizzato rivolgersi alla persona individuata dall'autorizzato stesso quale proprio fiduciario il quale provvederà all'inserimento della password.
- ❖ nei casi in cui sia necessario accedere ai dati personali attraverso il server, rivolgersi all'amministratore di sistema o provvedere, in collaborazione con l'amministratore di sistema stesso, alla creazione di credenziali di autenticazione da utilizzarsi esclusivamente per l'accesso da parte degli addetti alla manutenzione/gestione dei sistemi informatici.
- ❖ l'amministratore di sistema ha facoltà, in qualunque momento di controllare e verificare l'operato degli addetti alla manutenzione.
- ❖ qualora si renda necessario prelevare apparecchiature elettroniche per effettuare attività di ripristino o interventi di manutenzione che comportino il reset di password precedentemente individuate, la nuova password di accesso sarà comunicata al soggetto autorizzato il quale provvederà a cambiarla al termine delle operazioni di manutenzione.
- ❖ l'accesso al sistema informatico da parte degli addetti alla manutenzione/gestione del sistema è consentito unicamente previo inserimento di password e ID.
- ❖ è assolutamente vietato comunicare o diffondere i dati personali di qualsiasi natura provenienti dai database gestiti dalla Società, se non previa espressa comunicazione scritta.
- ❖ nel caso in cui ci si avvalga di soggetti esterni per interventi specialistici che comportino trattamento di dati personali deve essere rilasciata una dichiarazione scritta dell'intervento

effettuato che ne attesta la conformità alle disposizioni in materia di misure minime di sicurezza

8. NON OSSERVANZA DELLA NORMATIVA INTERNA. SANZIONI.

I soggetti autorizzati al trattamento, al fine di non esporre sé stessi e la Società a rischi sanzionatori, sono tenuti ad adottare comportamenti puntualmente conformi alla normativa vigente ed alla regolamentazione interna. È obbligatorio pertanto osservare le disposizioni portate a conoscenza con il presente Regolamento.
Il mancato rispetto o la violazione delle regole contenute nel presente Regolamento è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dal vigente CCNL nonché con le azioni civili e penali consentite.
Le disposizioni del presente Regolamento si applicano, per quanto compatibili, anche alle ipotesi di collegamento alla rete interna da postazioni esterne all'ufficio (ad es. collegamento da casa).
Sono fatte salve diverse disposizioni scritte eventualmente emanate dalla Società in attuazione della possibilità di smart working prevista dal modello di welfare aziendale per tempo vigente.

9. AGGIORNAMENTO E REVISIONE

Il presente Regolamento è soggetto, se necessario, a revisione con frequenza annuale. Il DPO, in quanto figura deputata anche all'aggiornamento della documentazione interna in materia di privacy, verifica costantemente la complessiva idoneità delle procedure predisposte al fine di assicurare il conseguimento degli obiettivi posti dalla disciplina vigente in materia, tenendo conto, in particolare, delle modifiche eventualmente intervenute nella normativa di riferimento, negli assetti organizzativi del Titolare nonché dell'efficacia dimostrata dalle procedure nella prassi applicativa.
Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento.
Le proposte verranno esaminate dal Titolare.

Data, 24.11.2022

per LIVENZA SERVIZI MOBILITA'
L'Amministratore unico pro tempore
Ing. Christian Lucchese

_____