REGISTRO DEI TRATTAMENTI

Redatto ai sensi dell'art. 30 del Regolamento Generale sulla Protezione dei Dati (GDPR) n.679/2016

Titolare del trattamento: **CASA FISCHER DI SERENI SILVA**

San Giuliano Terme, 17/09/2018

1. SCOPO DEL REGISTRO DEI TRATTAMENTI

Con il presente documento il Titolare del trattamento dei dati ottempera agli obblighi previsti all'art. 30 del Regolamento sul Trattamento di Dati e si impegna a provvedere al suo aggiornamento e mantenimento.

Il presente documento viene messo a disposizione di tutti i soggetti incaricati, interni ed esterni, al trattamento dei dati personali e tutti sono tenuti a rispettare quanto in esso previsto, al fine di salvaguardare il trattamento dei dati, intendendo per trattamento dei dati, così come disposto dall'art. 4: "*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*".

Il Registro dei Trattamenti contiene:

a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
b) le finalità del trattamento;
c) una descrizione delle categorie di interessati e delle categorie di dati personali;
d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

2. DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITA'

Il GDPR 679/2016 individua le seguenti figure.
Il **Titolare** è, secondo l'articolo 4 del suddetto regolamento, la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; nello specifico è la ditta **CASA FISCHER DI SERENI SILVA**

Per il trattamento dei dati personali il Titolare non ha nominato responsabili interni, assumendo direttamente l'incarico di progettare, realizzare e mantenere in efficienza le misure di sicurezza.

Inoltre, il Titolare ha individuato i seguenti ulteriori responsabili:

- **TOLAINI RICCARDO** responsabile esterno del trattamento dei dati, per la consulenza contabile

In ossequio al Provvedimento a carattere generale del Garante per la protezione dei dati personali del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relative alle attribuzioni delle funzioni di amministratore di sistema" il Titolare del trattamento non ha nominato nessun Amministratore di Sistema Gli eventuali problemi tecnici, sia hardware che software, sugli elaboratori vengono risolti da società esterne dietro chiamata a necessità

Nell'erogazione dei servizi e quindi per il trattamento dei dati personali, il Titolare **non si avvale di dipendenti o collaboratori**, di conseguenza non si applicano le disposizioni previste dal GDPR che disciplina che il trattamento venga effettuato solo da **soggetti che hanno ricevuto un formale incarico** mediante designazione per iscritto di ogni **singolo incaricato** con la quale si individua puntualmente l'ambito del trattamento consentito.

Qualora nel corso dello svolgimento delle attività lavorative, si rendesse necessario designare nuovi incaricati al trattamento, è opportuno compilare la tabella che segue:

Incaricati

3. TIPOLOGIE DEI DATI TRATTATI

A seguito dell'analisi compiuta si sono identificati i seguenti trattamenti:

- Dati **comuni** relativi al **personale**, necessari al rapporto di lavoro, alla reperibilità ed alla corrispondenza con gli stessi o richiesti ai fini fiscali e previdenziali o dati di natura bancaria, nonché di natura **particolare** conseguenti al rapporto di lavoro, ovvero inerenti i rapporti con gli enti previdenziali ed assistenziali, o l'adesione ad organizzazioni sindacali
- Dati **comuni** relativi a **fornitori** dagli stessi forniti, indispensabili allo svolgimento dei rapporti contrattuali, compresi i dati sulla situazione economica, o necessari per fini fiscali o afferenti alla reperibilità ed alla corrispondenza con gli stessi
- Dati **comuni** relativi a **clienti**, dagli stessi forniti, indispensabili allo svolgimento dei rapporti contrattuali, compresi i dati sul patrimonio e sulla situazione economica, o necessari per fini fiscali o afferenti alla reperibilità ed alla corrispondenza con gli stessi

4. ATTIVITA' DI TRATTAMENTO

Si riportano di seguito, in dettaglio, le attività di trattamento svolte:

TRATTAMENTO	FINALITA'	UFFICIO DI RIFERIMENTO	NATURA DEI DATI	CATEGORIA DI INTERESSATI	TITOLARE DEL TRATTAMENTO	INCARICATO AL TRATTAMENTO	INFORMATIVA	CONSENSO	TEMPO DI CONSERVAZIONE DEI DATI	TRASFERIMENTO DATI
RACCOLTA DATI ANAGRAFICI DEI FORNITORI	Registrazione e aggiornamento dei dati relativi ai fornitori	Ufficio amministrativo	☑ Comuni ☐ Genetici ☐ Biometrici ☐ Particolari ☐ Giudiziari	Fornitori	CASA FISCHER DI SERENI SILVA		Fornita in sede di richiesta di fornitura	Esonero ai sensi dell'art. 6 GDPR 679/2016	Come normativa di riferimento	☑ Non previsto ☐ Paesi UE ☐ Paesi Extra UE
RACCOLTA DATI ANAGRAFICI DEI CLIENTI	Registrazione e aggiornamento dei dati relativi ai clienti	Ufficio commerciale Ufficio amministrativo	☑ Comuni ☐ Genetici ☐ Biometrici ☐ Particolari ☐ Giudiziari	Clienti	CASA FISCHER DI SERENI SILVA		Fornita in sede di stipula di contratto	Esonero ai sensi dell'art. 6 GDPR 679/2016	Come normativa di riferimento	☑ Non previsto ☐ Paesi UE ☐ Paesi Extra UE
CONTRATTI	Adempimenti relativi alla gestione dei contratti	Ufficio commerciale Ufficio amministrativo	☑ Comuni ☐ Genetici ☐ Biometrici ☐ Particolari ☐ Giudiziari	Clienti - Fornitori	CASA FISCHER DI SERENI SILVA TOLAINI RICCARDO		Come da trattamento clienti e fornitori	Come da trattamento clienti e fornitori	Come normativa di riferimento	☑ Non previsto ☐ Paesi UE ☐ Paesi Extra UE
ORDINI EVASI	Fornitura di servizi e/o prodotti ai clienti	Ufficio commerciale Ufficio amministrativo	☑ Comuni ☐ Genetici ☐ Biometrici ☐ Particolari ☐ Giudiziari	Clienti	CASA FISCHER DI SERENI SILVA		Come da trattamento clienti	Come da trattamento clienti	Come normativa di riferimento	☑ Non previsto ☐ Paesi UE ☐ Paesi Extra UE
PREVENTIVI INVIATI	Gestione dei preventivi inviati	Ufficio commerciale amministrativo	☑ Comuni ☐ Genetici ☐ Biometrici ☐ Particolari ☐ Giudiziari	Potenziali clienti - clienti	CASA FISCHER DI SERENI SILVA		Come da trattamento clienti	Come da trattamento clienti	Come normativa di riferimento	☑ Non previsto ☐ Paesi UE ☐ Paesi Extra UE

TRATTAMENTO	FINALITA'	UFFICIO DI RIFERIMENTO	NATURA DEI DATI	CATEGORIA DI INTERESSATI	TITOLARE DEL TRATTAMENTO	INCARICATO AL TRATTAMENTO	INFORMATIVA	CONSENSO	TEMPO DI CONSERVAZIONE DEI DATI	TRASFERIMENTO DATI
PREVENTIVI RICEVUTI	Gestione dei preventivi ricevuti	Ufficio commerciale amministrativo	☑ Comuni ☐ Genetici ☐ Biometrici ☐ Particolari ☐ Giudiziari	Potenziali fornitori - fornitori	CASA FISCHER DI SERENI SILVA		Come da trattamento fornitori	Come da trattamento fornitori	Come normativa di riferimento	☑ Non previsto ☐ Paesi UE ☐ Paesi Extra UE
CONTABILITA'	Adempimenti relativi alla contabilità generale	Ufficio amministrativo	☑ Comuni ☐ Genetici ☐ Biometrici ☑ Particolari ☐ Giudiziari	Clienti e fornitori	CASA FISCHER DI SERENI SILVA TOLAINI RICCARDO		Come da trattamento clienti e fornitori	Come da trattamento clienti e fornitori	Come normativa di riferimento	☑ Non previsto ☐ Paesi UE ☐ Paesi Extra UE
CORRISPONDENZA	Archiviazione ordinata della corrispondenza	Segreteria	☑ Comuni ☐ Genetici ☐ Biometrici ☐ Particolari ☐ Giudiziari	Clienti fornitori e dipendenti			Come da trattamento clienti fornitori e dipendenti	Come da trattamento clienti fornitori e dipendenti	Come normativa di riferimento	☑ Non previsto ☐ Paesi UE ☐ Paesi Extra UE

5. MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE

Il trattamento dei dati avviene nella sede e luogo di lavoro, situata in via Pasteur, 18 Pontasserchio – San Giuliano Terme (PI).
L'accesso alla struttura è controllato attraverso una recinzione esterna.
La sede aziendale è un B&B composto da due camere, la sede è dotata di porte blindate e all'interno sono presenti armadi ignifughi. I dati vengono custoditi in un cassetto all'interno dell'abitazione del titolare.

Il trattamento avviene con i seguenti strumenti:

A – Schedari ed altri supporti cartacei
I supporti cartacei vengono ordinatamente raccolti in schedari, ovvero nella pratica cui si riferiscono, per essere archiviati, una volta terminato il ciclo lavorativo, in appositi armadi e in locali ai quali accedono solo le persone autorizzate, localizzati all'interno della sede lavorativa.

B – Elaboratori
Per elaboratori si intendono sia quelli non accessibili da altri elaboratori, terminali o, più in generale, da altri strumenti elettronici, sia quelli in rete privata, accessibili attraverso reti proprietarie, sulle quali possono viaggiare unicamente i dati del titolare del sistema, che in rete pubblica cioè quelli che utilizzano, anche solo per alcuni tratti, reti di telecomunicazione disponibili al pubblico, ivi inclusa la rete Internet.

L'entrata in vigore del Regolamento Europeo per la protezione dei dati ha reso obbligatorio l'adozione di una serie di misure atte a proteggere i personal computer sul quale avviene il trattamento dei dati presso ogni singolo ufficio. Le misure di sicurezza sono di seguito individuate.

- **Autenticazione informatica**: comprende i mezzi – siano essi programmi informatici o componenti hardware – deputati alla verifica ed alla convalidazione dell'identità di un dato soggetto. Ciò è possibile grazie all'utilizzo delle c.d. "credenziali di autenticazione" costituite da qualcosa che il soggetto incaricato "conosce" (ad esempio: un codice identificativo o una parola chiave), "possiede" (ad esempio: una smart card, un token), oppure "è" (ad esempio: una caratteristica biometrica, come l'impronta di un dito, del volto, della retina. Il sistema di autorizzazione: consente l'individuazione dei singoli trattamenti consentiti, andrà a costituire il c.d. "profilo di autorizzazione" del singolo incaricato, profilo che sarà sottoposto a verifica almeno una volta all'anno**.**
- **Adozione di idonei strumenti elettronici a protezione dei dati**
- **Aggiornamento del sistema anti – virus**
- **Back Up dei dati**: vi è l'obbligo di effettuare copie di back-up dei dati contenuti nei propri sistemi informatici.
- **Ripristino dati**: verificare periodicamente che il dato contenuto nella copia di back up sia realmente disponibile ed integro.
- **Adozione di tecniche di cifratura** per i dati idonei a rivelare lo stato di salute e la vita sessuale.

All'interno della sede è presente un solo PC son SO Windows 10 Home, munito di account personale protetto da password, lo stesso si collega ad internet tramite indirizzo IP dinamico (DHCP).
Per la protezione dello strumento è stato installato software antivirus e antimalware Windows Defender, inoltre è stato attivato il firewall integrato nel SO.
È presente inoltre una stampante collegata direttamente al computer, non sono presenti server e firewall fisici.

C – Impianti di video-sorveglianza
Non sono utilizzati impianti di video-sorveglianza.

6. ANALISI DEI RISCHI E MISURE ADOTTATE

6.1 COMPONENTI DEL RISCHIO

L'analisi dei possibili rischi che gravano sui dati è stata effettuata combinando due tipi di rilevazione:

- la tipologia dei dati trattati, la loro appetibilità, nonché la loro pericolosità per la privacy dei soggetti cui essi si riferiscono;
- le caratteristiche degli strumenti utilizzati per il trattamento dei dati.

Si stima il grado di rischio, che dipende dalla **tipologia dei dati trattati dal Titolare**, combinando il fattore della loro appetibilità per i terzi, con quello che esprime la loro pericolosità per la privacy del soggetto cui i dati si riferiscono:

	ELEVATISSIMO				
	ALTO	**1.** Dati comuni clienti			
GRADO DI INTERESSE PER I TERZI	**MEDIO**			**2.** Dati particolari personale	
	BASSO	**3.** Dati comuni di fornitori e terzi			
		BASSO	**MEDIO**	**ALTO**	**ELEVATISSIMO**
		PERICOLOSITA' PER LA PRIVACY DELL'INTERESSATO			

Si nota che un grado di rischio alto, è collegato al trattamento dei seguenti dati, alla tutela dei quali devono quindi essere dedicate particolari attenzioni:

- quelli idonei a rivelare informazioni di carattere particolare o giudiziario dei soggetti interessati o del personale, che sono accomunati dall'aspetto critico di avere un elevato grado di pericolosità per la privacy dei soggetti interessati;
- quelli che costituiscono una importante risorsa, commerciale e tecnologica, per il Titolare, in relazione ai danni che conseguirebbero da una eventuale perdita, o trafugamento, dei dati.

Per quanto concerne gli strumenti impiegati per il trattamento, le componenti di rischio possono essere idealmente suddivise in

1. rischio di area, che dipende dal luogo dove gli strumenti sono ubicati. Tale rischio è legato sostanzialmente:
   - al verificarsi di eventi distruttivi (incendi, allagamenti, corti circuiti)
   - alla possibilità che terzi malintenzionati accedano nei locali dove si svolge il trattamento (rapine, furti, danneggiamenti da atti vandalici)

2. rischio di guasti tecnici delle apparecchiature, che interessa in particolare gli strumenti elettronici (risorse hardware, software e supporti)

3. rischio di penetrazione logica nelle reti di comunicazione

4. rischio legato ad atti di sabotaggio e ad errori umani, da parte del personale appartenente all'organizzazione del Titolare, o di persone che con essa hanno stretti contatti

Alla luce dei fattori di rischio e delle aree individuate precedentemente, vengono descritte le misure atte a garantire:

- la **protezione delle aree e dei locali** ove si svolge il trattamento dei dati personali
- la **corretta archiviazione e custodia** di atti, documenti e supporti contenenti dati personali
- la **sicurezza logica**, nell'ambito degli strumenti elettronici

Le successive misure indicate a sostegno della fase di protezione dei dati si suddividono in

- misure già adottate al momento della stesura del presente documento
- ulteriori misure finalizzate ad incrementare il livello di sicurezza nel trattamento dei dati

6.2 LA PROTEZIONE DI AREE E LOCALI

Per quanto concerne il rischio che incombe sui locali ove si svolge il trattamento dei dati, sono previste le seguenti misure di sicurezza.

Rischio	**Probabilità**	**Gravità**
Accessi non autorizzati a locali ad accesso ristretto	Media	Media
Impatto sulla sicurezza: Accesso ai dati da parte di soggetti non autorizzati e/o accesso ai dati per trattamenti non consentiti		
Misure		
Porte blindate		

Rischio	**Probabilità**	**Gravità**
Accessi dei dipendenti fuori l'orario di lavoro	Media	Media
Impatto sulla sicurezza Accesso ai dati da parte di soggetti in orari non consentiti		
Misure		
Autorizzazione del Titolare		

Rischio	**Probabilità**	**Gravità**
Asporto materiale cartaceo destinato allo smaltimento rifiuti	Media	Alta
Impatto sulla sicurezza Accesso ai dati da parte di soggetti non autorizzati		
Misure		
Predisporre dispositivo distruggi documenti		
Riporre i documenti negli appositi sacchi di plastica, assicurare una chiusura ermetica degli stessi ed asportarli giornalmente		

Rischio	**Probabilità**	**Gravità**
Errori umani nella gestione della sicurezza fisica	Bassa	Media
Impatto sulla sicurezza Accesso ai dati da parte di soggetti non autorizzati e/o accesso ai dati per trattamenti non consentiti		
Misure		
Porte blindate		

Rischio	**Probabilità**	**Gravità**
Eventi distruttivi, naturali o artificiali, nonché dolosi, accidentali o dovuti ad incuria	Bassa	Alta
Impatto sulla sicurezza Distruzione totale o parziale dei dati e/o inibizione dell'accesso ai dati		
Misure		
Predisporre piano di Disaster Recovery		
Custodia in armadi/contenitori blindati e/o ignifughi dei dati e delle copie di sicurezza		

Rischio	**Probabilità**	**Gravità**
Guasto ai sistemi complementari	Bassa	Alta
Impatto sulla sicurezza Distruzione totale o parziale dei dati e/o inibizione dell'accesso ai dati		
Misure		
Predisporre sistemi UPS o generatori di corrente che garantiscono la continuità elettrica		

Rischio	**Probabilità**	**Gravità**
Sottrazione di strumenti contenenti dati	Bassa	Alta
Impatto sulla sicurezza Distruzione totale o parziale dei dati e/o diffusione non autorizzata di dati		
Misure		
Custodia in armadi/contenitori blindati e/o ignifughi dei dati e delle copie di sicurezza		

6.3 CUSTODIA E ARCHIVIAZIONE DEI DATI

Per la gestione, la custodia e l'archiviazione dei documenti e dei supporti, e sono state previste le seguenti misure idonee di sicurezza.

Rischio	**Probabilità**	**Gravità**
Accesso non autorizzato	Bassa	Media
Impatto sulla sicurezza Accesso ai dati per trattamenti non consentiti		
Misure		
Scelta di parole chiave che rispondono ai requisiti di sicurezza e che sono modificate ciclicamente		
Impostazioni in merito alla protezione dello strumento elettronico in caso di assenza temporanea durante le sessioni di lavoro		

Rischio	**Probabilità**	**Gravità**
Carenza di consapevolezza, disattenzione, incuria o indisponibilità	Bassa	Alta
Impatto sulla sicurezza Comportamenti contrari ai principi di sicurezza e protezione dei dati		
Misure		
Scelta di metodi sicuri finalizzati al controllo e alla custodia dei documenti contenenti dati personali per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento senza l'ausilio di strumenti elettronici		
Adozione di procedure per le copie di sicurezza, la loro custodia ed il ripristino della disponibilità dei dati		

Rischio	**Probabilità**	**Gravità**
Comportamenti sleali o fraudolenti	Minima	Alta
Impatto sulla sicurezza Accesso ai dati per trattamenti non consentiti e/o contrari ai principi di sicurezza e protezione dei dati		
Misure		
Definizione di responsabilità e sanzioni disciplinari		
Controllo degli accessi ai dati e programmi		
Monitoraggio continuo delle sessioni di lavoro		

Rischio	**Probabilità**	**Gravità**

Errore materiale	Media	Media
Impatto sulla sicurezza Operazioni accidentali non consentite e/o contrarie ai principi di sicurezza e protezione dei dati		
Misure		
Reinstallazione dei programmi danneggiati o distrutti		
Definizione di procedure per le copie di sicurezza, la loro custodia e il ripristino dei dati		

Rischio	**Probabilità**	**Gravità**
Sottrazione di credenziali di autenticazione	Bassa	Alta
Impatto sulla sicurezza Accesso ai dati da parte di soggetti non autorizzati e/o accesso ai dati per trattamenti non consentiti		
Misure		
Istruzioni in merito alla segretezza e alla custodia delle credenziali di autenticazione		
Aggiornamento periodico delle credenziali di autenticazione		

6.4 MISURE LOGICHE DI SICUREZZA

Per il trattamento effettuato con strumenti elettronici si sono individuate le seguenti misure:

- realizzazione e gestione di un **sistema di autenticazione informatica** al fine di accertare l'identità delle persone che hanno accesso agli strumenti elettronici
- **protezione di strumenti e dati** da malfunzionamenti e attacchi informatici
- prescrizione delle opportune cautele per la custodia e l'utilizzo dei **supporti rimovibili**, contenenti dati personali

6.5 SISTEMA DI AUTENTICAZIONE INFORMATICA

Il **sistema di autenticazione informatica** viene adottato per disciplinare gli accessi a tutti gli strumenti elettronici, presenti nell'organizzazione del Titolare, fatta unicamente salva l'eventuale eccezione per quelli che:

- non contengono dati personali;
- contengono solo dati personali destinati alla diffusione, che sono quindi per definizione conoscibili da chiunque.

L'eccezione vale, ovviamente, solo per gli strumenti elettronici che non siano in rete, o che siano in rete esclusivamente con strumenti elettronici non contenenti dati personali, o contenenti solo dati personali destinati alla diffusione.

Per tutti gli altri casi, è impostata e gestita una procedura di autenticazione, che permette di verificare l'identità della persona, e quindi di accertare che la stessa è in possesso delle **credenziali di autenticazione** per accedere ad un determinato strumento elettronico.

Per **realizzare** le credenziali di autenticazione si utilizza il seguente metodo:

- si associa un codice per l'identificazione (*username)* ad una parola chiave riservata (*password*), conosciuta solamente dal Titolare, che provvederà ad elaborarla, mantenerla riservata e modificarla periodicamente.

Per l'**attribuzione e la gestione delle credenziali per l'autenticazione** si utilizzano i seguenti criteri:

- ad ogni incaricato esse vengono assegnate o associate individualmente, per cui non è ammesso che due o più incaricati possano accedere agli strumenti elettronici utilizzando la medesima credenziale;
- è invece ammesso, qualora sia necessario o comunque opportuno, che ad una persona venga assegnata più di una credenziale di autenticazione.

Al verificarsi dei seguenti casi, è prevista la disattivazione delle credenziali di autenticazione:

- immediatamente, nel caso in cui l'incaricato perda la qualità, che gli consentiva di accedere allo strumento.

Agli incaricati vengono impartite precise istruzioni in merito ai seguenti punti:

- dovere di **custodire i dispositivi**, attribuiti agli incaricati a titolo di possesso ed uso esclusivo, con i quali si può accedere agli strumenti informatici (ad esempio, il tesserino magnetico o la smart card): la custodia deve avvenire in modo diligente, sia nell'ipotesi in cui tali dispositivi siano riposti negli uffici, che in quella in cui l'incaricato provveda a portare il dispositivo con sé (viene prescritto l'obbligo di custodirlo diligentemente). In ipotesi di smarrimento, l'incaricato deve provvedere immediatamente a segnalare la circostanza al Titolare del trattamento, o alle altre persone che sono state a tale fine indicate, al momento dell'attribuzione del dispositivo
- obbligo di **non lasciare incustodito e accessibile lo strumento elettronico**, durante una sessione di trattamento, neppure in ipotesi di breve assenza
  - dovere di **elaborare in modo appropriato la password**, e di **conservare la segretezza** sulla stessa, nonché sulle altre componenti riservate della credenziale di autenticazione (username). Agli incaricati è imposto l'obbligo di provvedere a modificare la password ciclicamente.

  Le **password** sono composte da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non permetta una tale lunghezza, da un numero di caratteri pari al massimo consentito dallo strumento stesso.

Agli incaricati è prescritto di utilizzare alcuni accorgimenti, nell'elaborazione delle password:

- esse non devono contenere riferimenti agevolmente riconducibili all'interessato (non solo nomi, cognomi, soprannomi, ma neppure date di nascita proprie, dei figli o degli amici), né consistere in nomi noti, anche di fantasia (pippo, pluto, paperino, ….)

La password non deve essere comunicata a nessuno (non solo a soggetti esterni, ma neppure a persone appartenenti all'organizzazione, siano esse colleghi, responsabili del trattamento, amministratore del sistema o titolare). Nei casi di prolungata assenza o impedimento dell'incaricato, che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, potrebbe però rendersi necessario disporre della password dell'incaricato, per accedere agli strumenti ed ai dati. A tale fine, agli incaricati sono state fornite istruzioni scritte, affinché essi:

- scrivano la parola chiave su un foglio di carta, da inserire in una busta che deve essere chiusa e sigillata
- consegnino la busta a chi custodisce le copie delle parole chiave, il cui nominativo viene loro indicato al momento dell'attribuzione della password

Solo al verificarsi delle condizioni, sopra esposte, che rendono necessario accedere allo strumento elettronico, utilizzando la copia della parola chiave, il titolare o un responsabile potranno richiedere la busta che la contiene, a chi la custodisce. Dell'accesso effettuato si dovrà provvedere ad informare, tempestivamente, l'incaricato cui appartiene la parola chiave.

6.5.1 TIPOLOGIE DI DATI AI QUALI GLI INCARICATI POSSONO ACCEDERE

Per quanto concerne le **tipologie di dati ai quali gli incaricati possono accedere**, ed i trattamenti che possono effettuare, si osserva che per gli incaricati sono previsti profili di autorizzazione distinti, in virtù del fatto che ciascuno può avere un accesso ai dati differenziato in base al ruolo/mansione ricoperto in ditta

Le autorizzazioni all'accesso vengono rilasciate e revocate dal titolare e, se designato, dal responsabile, ovvero da soggetti da questi appositamente incaricati.

Il profilo di autorizzazione non viene in genere studiato per ogni singolo incaricato, ma è generalmente impostato per classi omogenee di incaricati (ad esempio, attribuendo un determinato profilo di autorizzazione a tutti gli impiegati della contabilità, ed attribuendone un altro a coloro che lavorano nell'ufficio personale L'obiettivo di fondo, in ogni caso, è di limitare preventivamente l'accesso, di ciascuna classe omogenea di incaricati, ai soli dati necessari per effettuare le operazioni di trattamento, che sono indispensabili per svolgere le mansioni lavorative.

Periodicamente, e comunque almeno annualmente, viene verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione: ciò per quanto riguarda l'ambito di trattamento consentito sia ai singoli incaricati, che agli addetti alla manutenzione e gestione degli strumenti elettronici.

6.5.2 PROTEZIONE DI STRUMENTI E DATI

Per quanto riguarda la **protezione di strumenti e dati**, da malfunzionamenti, attacchi informatici e programmi che contengono virus e malware, vengono adottate le misure sotto descritte.

Il primo aspetto riguarda la protezione dei dati personali dal rischio di intrusione e dall'azione di programmi di cui all'articolo 615-quinquies del codice penale, aventi per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento (comunemente conosciuti come virus).

A tale fine, si è dotati di idonei strumenti elettronici e programmi che, in relazione alla continua evoluzione tecnologica, si è ritenuto opportuno di sottoporre ad aggiornamento continuo.

Il secondo aspetto riguarda la protezione degli elaboratori in rete dall'accesso abusivo, di cui all'articolo 615-ter del codice penale, ai sensi del quale compie tale reato chi si introduce abusivamente in un sistema informatico o telematico, protetto da misure di sicurezza, ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo.
La protezione da tali accessi, avviene mediante l'impiego di idonei strumenti elettronici, comunemente conosciuti come firewall.

A tale riguardo l'organizzazione si è da tempo dotata di tali strumenti, per la protezione degli elaboratori in rete.

Per di più, si è data disposizione di provvedere periodicamente alla pulizia dei file, all'eliminazione dei cookies, alla cancellazione della cronologia, alla pulizia interna dell'hardware.

6.5.3 SUPPORTI RIMOVIBILI

Per quanto concerne i **supporti rimovibili** (es. HD esterno, CD/DVD, chiavette USB….), contenenti dati personali, la norma impone particolari cautele solo nell'ipotesi in cui essi contengano dati particolari o giudiziari.

L'organizzazione ha ritenuto di estendere tali precetti ai supporti contenenti dati personali di qualsiasi natura, anche comune, prescrivendo agli incaricati del trattamento quanto segue:

- i supporti devono essere custoditi ed utilizzati in modo tale da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti: in particolare, essi devono essere conservati in cassetti chiusi a chiave, durante il loro utilizzo, e successivamente formattati, quando è cessato lo scopo per cui i dati sono stati memorizzati su di essi;
- una volta cessate le ragioni per la conservazione dei dati, si devono in ogni caso porre in essere gli opportuni accorgimenti, finalizzati a rendere inintelligibili e non ricostruibili tecnicamente i dati contenuti nei supporti. Tali dati devono quindi essere cancellati, se possibile, e si deve arrivare addirittura a distruggere il supporto, se necessario per i fini in esame.

Per il trattamento effettuato con strumenti elettronici, dunque, si sono individuate le seguenti misure:

Rischio	**Probabilità**	**Gravità**
Accessi esterni non autorizzati	Media	Media
Impatto sulla sicurezza Accesso agli strumenti per operazioni non consentite / non autorizzate		
Misure		
Presenza di un sistema di autenticazione delle credenziali per tutti gli accessi agli archivi elettronici		
Attivazione di uno screensaver automatico dopo pochi minuti di non utilizzo, con inserimento password per la prosecuzione del lavoro		
Disattivazione delle credenziali di autenticazione nel caso di inutilizzo perdurato		
Distruzione di tutti i supporti removibili non utilizzati		
Utilizzo di un sistema Firewall sugli elaboratori		

Rischio	**Probabilità**	**Gravità**
Azione di virus informatici o di programmi suscettibili di recare danno	Alta	Alta
Impatto sulla sicurezza Distruzione totale o parziale e/o diffusione non autorizzata e/o inibizione dell'accesso ai dati		
Misure		
Utilizzo di un sistema antivirus		
Aggiornamento periodico dei programmi antivirus		
Aggiornamento periodico dei programmi per elaboratore contro la vulnerabilità dei dati		

Rischio	**Probabilità**	**Gravità**
Intercettazione di informazioni in rete	Alta	Alta
Impatto sulla sicurezza Diffusione non autorizzata di dati		
Misure		
Sistema di protezione dei dati trasmessi: Crittografia e/o Cifratura e/o Certificato digitale e/o ID digitale		
Controlli periodici sul sistema di protezione nella trasmissione dei dati		

Rischio	**Probabilità**	**Gravità**
Malfunzionamento, guasti, eventi naturali, alterazioni delle trasmissioni, indisponibilità o degrado degli strumenti	Media	Media
Impatto sulla sicurezza Distruzione totale o parziale dei dati e/o inibizione dell'accesso ai dati		
Misure		
Manutenzione programmata degli strumenti		
Controllo sull'operato degli addetti alla manutenzione		
Definizione di procedure per le copie di sicurezza, la loro custodia e il ripristino dei dati		
Istruzioni organizzative e tecniche per la custodia dei supporti removibili su cui sono memorizzati i dati		
Predisporre sistemi UPS o generatori di corrente che garantiscono la continuità elettrica		

Rischio	**Probabilità**	**Gravità**
Spamming o tecniche di sabotaggio	Alta	Media
Impatto sulla sicurezza Distruzione totale o parziale e/o diffusione non autorizzata e/o inibizione dell'accesso ai dati		
Misure		
Utilizzo di un sistema Firewall sugli elaboratori		
Aggiornamento periodico del sistema Firewall		
Controllo degli accessi a siti internet non sicuri		
Divieto di scaricare software e di installare programmi da siti poco attendibili o non ufficiali		
Disposizione di tenere sempre attiva l'opzione del browser "**richiedi conferma**" per l'installazione e il download di oggetti sulla propria macchina		
Protezione della posta elettronica con disposizione di verifica della provenienza delle e-mail e di non esecuzione dei file allegati ai messaggi senza preventiva scansione antivirus		
Utilizzo della casella di posta elettronica dell'ufficio come strumento di lavoro e dunque esclusivamente per esigenze lavorative		

Le misure logiche di sicurezza, di cui è dotato il Titolare per la protezione dei trattamenti che avvengono con strumenti elettronici appaiono nel loro complesso soddisfacenti, al fine di garantire la necessaria sicurezza ai dati personali trattati.

6.6 CRITERI E MODALITA' DI RIPRISTINO DATI

Per i dati trattati con strumenti elettronici sono previste procedure di backup attraverso le quali viene periodicamente effettuata una copia di tutti i dati presenti nel sistema, in modo da permettere la ricostruzione dei dati a fronte di cancellazioni o danneggiamenti. Gli incaricati per iscritto, che hanno il compito di svolgere le operazioni di trattamento, debbono custodire e controllare i supporti su cui sono registrati i dati in maniera che soggetti non autorizzati non possano venire a conoscenza, nemmeno accidentalmente dei contenuti di tali supporti. Tali supporti non possono essere utilizzati da altri soggetti che non possiedono l'incarico scritto di poterli trattare. Gli incaricati sono formati per un efficace sistema di salvataggi personali, tali da evitare perdite accidentali dovute a guasti o all'azione di programmi dannosi (virus).

Le copie vengono chiuse in un cassetto e custodite in luoghi protetti in luoghi diversi dalla sede. Si è data disposizione di verificare, effettuato il backup, la leggibilità del supporto e che una volta a settimana si proceda a verifica a campione della leggibilità dei dati e che ogni volta venga distrutto il precedente backup.

COPIE DI SICUREZZA E RIPRISTINO DATI

Responsabile Copie
SERENI SILVA

Strutture di conservazione delle copie di sicurezza
All'esterno della sede

Copie di sicurezza
Viene eseguita n. 1 copia su USB.

7. COMPLIANCE AL GDPR

Il processo di adeguamento al GDPR effettuato dal Titolare del trattamento non ha evidenziato problematiche particolari.
I dati trattati dall'azienda sono limitati a quelli necessari alla gestione aziendale, non effettua attività di marketing nei confronti dei clienti finali e non ha un sistema di videosorveglianza.
L'azienda ha un sito web dove è presente un modulo di registrazione corredato da apposita informativa, ha delle pagine social aziendali ma con effettua acquisizione di dati limitandosi alla pubblicazione di news ed eventi.

La valutazione dei rischi effettuata non evidenzia dei trattamenti per i quali è necessario effettuare una DPIA.

Il processo di compliance al GDPR richiede una valutazione periodica dei trattamenti, che sarà effettuata dal Titolare implementando il registro dei Trattamenti.