SOCIETA' LEOMIND S.R.L.

VIALE CAVOUR 78, SALSOMAGGIORE TERME (PR) 43039
Website: GECOTRUCK.it
PEC:LEOMIND@pec.it
E-Mail: info@gecotruck.it

MODELLO ORGANIZZATIVO PRIVACY privacy policy

Questa Policy assicura regole e linee guida per la gestione del trattamento dei dati personali, per la conformità al Regolamento Generale Europeo sulla Protezione dei Dati 679/2016 (G.D.P.R.) ai sensi dell'art. 25 e delle normative locali che disciplinano la materia.

Documentazione redatta in ottemperanza a quanto disposto dal GDPR 2016/679 "Regolamento generale sulla protezione dei dati". al D. lgs. 196/2003 "Codice in materia di protezione dei dati" e s.m.i. e ai Provvedimenti del Garante per la protezione dei dati personali

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Stato delle revisioni

Versione	Data	Descrizione	Autore
00	*01/10/2025*	Prima emissione	Studio legale Avv. Cinque
01	_____	Aggiornamento elenco dei documenti	D.P.O.
02	_____	Aggiornamento modello organizzativo privacy	D.P.O.
03	_____	Aggiornamento mappatura dei rischi	D.P.O.
	–		

Sommario

Finalità Privacy Policy Group 3
Quadro normativo di riferimento 5
Glossario del regolamento UE 679/2016 6
Informazioni identificative aziendali 9
Referenti 9
Informazioni caratteristiche 9
Profili Soggettivi 10
Titolare 10
Responsabili del trattamento 11
Responsabile al Trattamento 11
Amministratori di sistema 13
Autorizzati al trattamento 13
Principi privacy generali 17
Mappa delle tipologie dei trattamenti assegnati alle funzioni 21
Analisi Dei Rischi e Sistema di Sicurezza 23
Misure Di Sicurezza 25
Misure di sicurezza generali sede operativa in Salsomaggiore Terme (PR). 27
Misure di sicurezza di area 28
Elenco documenti 31

Finalità Privacy Policy Group

Nell'ambito dello svolgimento della propria attività imprenditoriale, la società LEOMIND s.r.l. raccoglie dati personali e informazioni riservate, che si impegna a trattare in ottemperanza a tutte le leggi in materia di privacy e riservatezza vigenti nelle giurisdizioni in cui opera.

In particolare, LEOMIND s.r.l si impegna a prestare la massima diligenza nella raccolta dei dati personali e nella loro conservazione; a utilizzare nel trattamento dei dati gli strumenti tecnicamente più idonei e ogni misura e precauzione necessaria e opportuna per garantire la sicurezza e la riservatezza dei suddetti dati; a non comunicare o in qualsiasi modo diffondere a terzi non autorizzati i dati personali di cui sia venuto a conoscenza nello svolgimento della propria attività.

Lo stesso impegno di riservatezza nell'utilizzo, nell'elaborazione e nella custodia dei dati, deve essere assunto e garantito da tutto il personale dipendente e non che, nell'esercizio delle proprie attività, effettua il trattamento di dati personali per conto della LEOMIND s.r.l

I dipendenti e i collaboratori della LEOMIND s.r.l, a tutti i livelli, sono pertanto tenuti a riconoscere se stanno raccogliendo, utilizzando, elaborando, conservando o condividendo dati personali oggetto di tutela.

Il rispetto di tali principi è responsabilità del Titolare del trattamento e comporta una valutazione, una gestione e un monitoraggio continuo del rischio.

Tutti i dipendenti/collaboratori della LEOMIND s.r.l sono responsabili del rispetto dei principi e delle regole definite nel presente documento.

L'osservanza delle disposizioni della presente Policy deve considerarsi parte essenziale delle obbligazioni contrattuali dei dipendenti/collaboratori.

Le violazioni della presente Policy possono condurre ad un'azione disciplinare inclusi – nei casi più gravi – il licenziamento, nel rispetto delle leggi vigenti e dei contratti di lavoro nazionali, o la cessazione del rapporto di collaborazione (per i soggetti terzi).

Abbiamo definito un adeguato MODELLO ORGANIZZATIVO PRIVACY (M.O.P.) con il quale abbiamo introdotto il controllo delle misure tecniche ed organizzative finalizzate a garantire il rispetto dei principi che diffondiamo a tutti coloro che operano nei nostri processi e nel rispetto del Regolamento UE 679/2016 G.D.P.R. e della legislazione applicabile ai trattamenti effettuati.

La presente policy definisce le modalità di adozione dei criteri di sicurezza in merito alla raccolta, trattamento e protezione dei dati identificativi degli interessati (persone fisiche) con le quali interagiamo nel nostro lavoro, oltre a definire le modalità di progettazione, valutazione, implementazione, controllo e aggiornamento delle misure di sicurezza poste a protezione dei dati personali fin dalle fasi di sviluppo e progettazione (PRIVACY BY DESIGN) e nonché nell'adozione di configurazioni predefinite (PRIVACY BY DEFAULT).

Ogni trattamento di dati personali avviene nel rispetto primario dei seguenti principi di ordine generale:

1. **i dati sono trattati**:
    a. secondo il principio di liceità, vale a dire conformemente alle disposizioni del GDPR e della normativa vigente in materia di privacy e data protection, nonché alle disposizioni del Codice civile, per cui, più in particolare, il trattamento non è contrario a norme imperative, all'ordine pubblico ed al buon costume;
    b. secondo il principio fondamentale di correttezza, il quale deve ispirare chiunque tratti qualcosa che appartiene alla sfera altrui;
2. **i dati sono raccolti solo per scopi**:
    a. determinati, vale a dire che non è consentita la raccolta come attività fine a sé stessa;
    b. espliciti, nel senso che il soggetto interessato viene informato sulle finalità del trattamento;

c. legittimi, cioè, oltre al trattamento, come è evidente, anche il fine della raccolta dei dati deve essere lecito;
d. compatibili con il presupposto per il quale sono inizialmente trattati, specialmente nelle operazioni di comunicazione e diffusione degli stessi;

3. **i dati inoltre sono**:
   a. esatti, cioè, precisi e rispondenti al vero e, se necessario, aggiornati;
   b. pertinenti, ovvero, il trattamento è consentito soltanto per lo svolgimento delle funzioni istituzionali, in relazione all'attività che viene svolta;
   c. completi: non nel senso di raccogliere il maggior numero di informazioni possibili, bensì di contemplare specificamente il concreto interesse e diritto del soggetto interessato;
   d. non eccedenti in senso quantitativo rispetto allo scopo perseguito, ovvero devono essere raccolti solo i dati che siano al contempo strettamente necessari e sufficienti in relazione al fine, cioè la cui mancanza risulti di ostacolo al raggiungimento dello scopo stesso;
   e. conservati per un periodo non superiore a quello necessario per gli scopi del trattamento e comunque in base alle disposizioni aventi ad oggetto le modalità ed i tempi di conservazione degli atti amministrativi. Trascorso detto periodo i dati sono resi anonimi o cancellati e la loro comunicazione e diffusione non è più consentita.

Il Documento traccia anche il profilo delle vulnerabilità più diffuse mirando a soddisfare tutte le misure di sicurezza organizzative, fisiche e logiche previste dalla normativa contenuta nel GDPR 2016/679.

In sintesi, le tre macroaree di sicurezza, che verranno analizzate e specificate nei documenti allegati che compongo il nostro Modello Operativo Privacy si possono così identificare:

Sicurezza Fisica: la funzione svolta dalla sicurezza fisica è quella di apprestare tutti i mezzi e gli strumenti necessari per proteggere persone, cose e ambienti dai suddetti rischi. Si suddivide in sicurezza dell'area preordinata ad evitare accessi fisici non autorizzati e sicurezza delle apparecchiature hardware preordinata alla protezione da manomissione o furti dell'hardware e comprende anche la manutenzione degli stessi;

Sicurezza Logica: la funzione svolta dalla sicurezza logica è quella di proteggere i "dati" attraverso misure di sicurezza di carattere tecnologico (c.d. Information and Communication Technology). Rientrano in questa area i c.d. Sistemi di sicurezza preordinati alla protezione di tutte le piattaforme dati presenti in azienda (in primis mediante autenticazione e controllo accessi); meccanismi di sicurezza preordinati alla creazione del *modus operandi* dei sistemi di sicurezza (cifratura, firma digitale, meccanismi per l'autenticazione ecc.)

Sicurezza Organizzativa: la funzione svolta dalla sicurezza organizzativa è quella di prevedere regole e procedure finalizzate a disciplinare gli aspetti organizzativi del processo di sicurezza fisica e logica. In questa area rientrano tutte le prescrizioni riguardanti la definizione dei ruoli, la distribuzione dei compiti e delle responsabilità. Quindi a titolo esemplificativo rientrano in questa area tutte le procedure relative alla gestione delle contromisure di sicurezza logica; oppure le procedure di gestione per la sicurezza della rete, le procedure riguardanti il personale, le procedure di aggiornamento dei software, le procedure di backup, le procedure di formazione degli incaricati e dei responsabili ecc.…

Conclusioni
Tutti i principi sono condivisi con il personale che, oltre ad impegnarsi per la corretta gestione del Sistema, fornisce anche degli stimoli alla Direzione per l'implementazione ed il miglioramento continuo dello stesso.

Quadro normativo di riferimento

- **Regolamento (Ue) 679/2016** *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*
- **D. Lgs. 196/2003** *Codice in materia di trattamento dei dati personali*
- **D. Lgs. 101/2018** *Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).*
- **D. Lgs. 33/2013** *Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni (titolo così sostituito dall'art. 1, comma 1, d.lgs. n. 97 del 2016)*
- **Legge 300/1970** *Statuto dei Lavoratori" così modificata e integrata dal D. Lgs 151/2015*
- **Nuove disposizioni normative sulle attività di call center Articolo 1, comma 243, della Legge n. 232 del 2016** *(c.d. legge di bilancio) che sostituisce l'art. 24 -bis, D.L. 22/06/2012, n. 83 convertito con modificazioni dalla legge 07/08/2012, n. 134/2012*
- **Provvedimento dell'Autorità Garante del 27 novembre 2008** *Misure e accorgimenti prescritti ai Titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema*
- **Provvedimento dell'Autorità Garante del 8 aprile 2010** *Provvedimento in materia di videosorveglianza*
- **Provvedimento dell'Autorità Garante del 8 ottobre 2011 nr. 370** *Sistemi di localizzazione dei veicoli nell'ambito del rapporto di lavoro*
- **Provvedimento dell'Autorità Garante del 13 luglio 2016 nr. 303** *Trattamento di dati personali dei dipendenti mediante posta elettronica e altri strumenti di lavoro*
- **Provvedimento dell'Autorità Garante del 30 aprile 2019** *Data breach*
- **Provvedimento dell'Autorità Garante del 27 novembre 2008 [doc. web n. 1577499]** *Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*
- **Provvedimento dell'Autorità Garante del 25 giugno 2009 [doc. web n. 1626595]** *Modifiche del provvedimento del 27 novembre 2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga dei termini per il loro adempimento*
- **Linee guida 3/2019** *EDPB sul trattamento dei dati personali attraverso dispositivi video*
- **Linee guida del Garante** *maggiori garanzie sul posto di lavoro - 13 dicembre 2006*
- **Linee guida del Garante** *per posta elettronica ed internet - 5 marzo 2007*
- **Linee guida del Garante** *in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali - 26 luglio 2012*
- **Semplificazioni delle misure di sicurezza - 27 novembre 2008**
- **Rifiuti di apparecchiature elettrice ed elettroniche e misure di sicurezza dei dati personali- 13 ottobre 2008**
- **Legge 18 marzo 2008 sui crimini informatici**

Glossario del regolamento UE 679/2016

1. «**dato personale**»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere 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;
2. «**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;
3. «**limitazione di trattamento**»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
4. «**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;
5. «**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;
6. «**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;
7. «**titolare del trattamento**»: 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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
8. «**responsabile del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
9. «**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;
10. «**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;
11. «**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;
12. «**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;
13. «**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;

14. «**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;
15. «**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;
16. «**stabilimento principale**»:
    a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;
    b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;
17. «**rappresentante**»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;
18. «**impresa**»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;
19. «**gruppo imprenditoriale**»: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;
20. «**norme vincolanti d'impresa**»: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;
21. «**autorità di controllo**»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;
22. «**autorità di controllo interessata**»: un'autorità di controllo interessata dal trattamento di dati personali in quanto:
    il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;
    a) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure
    b) un reclamo è stato proposto a tale autorità di controllo;
23. «**trattamento transfrontaliero**»:
    a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure
    b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;
24. «**obiezione pertinente e motivata**»: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione

dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;

25. «**servizio della società dell'informazione**»: il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio;
26. «**organizzazione internazionale**»: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

Informazioni identificative aziendali

Azienda	LEOMIND s.r.l		
sede legale	VIALE CAVOUR 78, SALSOMAGGIORE TERME (PR) 43039		
Sede operativa	VIALE CAVOUR 78, SALSOMAGGIORE TERME (PR) 43039		
Attività	SVILUPPO SOFTWARE PER L'AUTOTRASPORTO E SERVIZI TECNOLOGICI CONNESSI		
Telefono		**E-mail**	
PEC	LEOMIND@PEC.IT	**P. iva**	03126740343

Referenti

Nome	LEOMIND S.r.l.	**Ruolo**	A.D. titolare trattamento
E-mail		**Cell. /tel.**	
Nome	Dot. Marco Scala	**Ruolo**	D.P.O. – RESPONSABILE PRIVACY
E-mail		**Cell. /tel.**	

Informazioni caratteristiche

Tipologia interessati	☒ **Clienti persone fisiche**	☐ ~~**Potenziali clienti privati**~~	☒ **Fornitori**	☒ **Potenziali Fornitori**	☐ ~~Minori~~
	☒ **Clienti aziende/enti**	☐ Potenziali Clienti aziende/enti	☒ **Candidati**	☒ **Enti pubblici**	
	☒ **Collaboratori (stagisti, interinali, apprendisti)**	☒ **Dipendenti**	☒ **Utenti web**	☐ clienti web (e-commerce)	

Videosorveglianza	☐ Nessun sistema	☒ **Videocamere con registrazione varchi di accesso**	☐ Videocamere aree frequentate da dipendenti	☒ **Videocamere aree frequentate da clienti e da dipendenti**	☐ Solo videocitofoni

Sito web	☐ Nessun sito web	☒ **Sito web: http://www.GECOTRUCK.it**	☒ **Form contatto**	☒ **accesso login**
e-commerce	☐ portale e-commerce dedicato	☒ area dedicata nel sito principale	☐ area in market place	

Tipologie dei dati trattati	☒ **nome cognome**	☒ **e-mail**	☒ **indirizzo**	☒ **numero telefono fisso**	☒ **numero telefono mobile**
	☒ **cod. fiscale**	☒ **dati assicurativi**	☒ **numero di targa del veicolo**	☒ **numero di patente**	
	☐ numeri di carta di credito	☒ **numero carta identità e patente**	☒ **data di nascita**	☒ **luogo di nascita**	
	☒ **dati bancari**	☒ **indirizzo IP**	☒ ~~**dati di solvibilità economica**~~	☒ **immagini e/o video**	
	☒ **dati sensibili:** **- dati che rivelano la professione** **- dati assicurativi** **- dati della patente** **- dati che rilevano i punti patente e Cqc** **- dati tachigrafici** **- dati sulla posizione dei veicoli in tempo reale** DATI PARTICOLARI (art. 9 GDPR) ~~- dati che rivelano l'origine razziale o etnica~~ ~~- dati che rivelano le opinioni politiche~~ ~~- dati che rivelano le convinzioni religiose~~ ~~- dati che rivelano l'appartenenza sindacale~~ ~~- dati biometrici~~ ~~- dati relativi alla salute~~ ~~- dati relativi alla vita/orientamento sessuale~~		**Altri dati:** GIUDIZIARI (art. 10 GDPR) ~~1. dati relativi a indagini penali in corso~~ ~~2. dati relativi a condanne penali~~ ~~3. dati relativi a carichi pendenti~~ ~~4. dati relativi a casellario giudiziale~~		
	☐ ~~invio newsletter marketing~~ a clienti	☐ ~~invio newsletter marketing~~ a potenziali clienti	☐ ~~archivi con elenchi di~~ potenziali clienti aziende	☐ ~~archivi con elenchi di~~ potenziali clienti privati	

Attività marketing	☐ marketing di affiliazione con fidelity card	☐ archivi con elenchi di potenziali clienti aziende	☐ sistemi automatizzati di profilazione con dati provenienti dagli acquisti
NOTE	**Le tipologie di dati trattati, si riferiscono alla totalità della tipologia degli interessati (clienti – fornitori – enti – dipendenti – persone fisiche che a vario titolo vengono coinvolte nell'attività del titolare)**		

Profili Soggettivi

Titolare

Secondo le definizioni contenute nel GDPR (articolo 4 n. 7) il Titolare è 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 per finalità lecite, come previsto dall'art. 6 e ne decide le modalità di trattamento [….]; si tratta, della figura che è all'origine del trattamento.

Questo implica, conseguentemente, che, seppure declinata attraverso un sistema di ruoli e responsabilità dei diversi soggetti, la capacità dell'azienda di dare puntuale adempimento alle prescrizioni imposte dal GDPR dipende dalla capacità di ciascun componente dell'organizzazione di assumere, in modo consapevole e responsabile, le decisioni di competenza e intraprendere le conseguenti azioni.

Sulla base di tale definizione - tenuto conto dell'attività di assessment di Gruppo svolta sulla tipologia dei dati personali trattati, sui trattamenti infragruppo, sui processi organizzativi, sui presidi tecnologici, nonché sui processi decisionali centralizzati a livello di HQ – si è ritenuto che in via generale e salvo eccezioni lo Stabilimento principale[1], ove sono prese le decisioni che riguardano trattamenti di dati personali, corrisponde alla sede operativa della **LEOMIND s.r.l. in** VIALE CAVOUR 78, SALSOMAGGIORE TERME (PR) 43039
Presso la sede operativa sono, infatti, effettivamente assunte le principali decisioni sulle finalità e sui mezzi del trattamento e indipendentemente dal fatto che i dati siano trattati presso quella sede[2].

È riconosciuta al Titolare del trattamento, nella persona del legale rappresentante pro tempore, la possibilità di prevedere, sotto la propria responsabilità, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a soggetti espressamente delegati, che operino sotto la sua autorità.

Il titolare del trattamento, secondo le responsabilità declinate nel GDPR:

- designa tramite atto formale il responsabile della protezione dei dati, ne pubblica i dati di contatto e li comunica all'autorità di controllo (art 37 Designazione del responsabile della protezione dei dati),
- mette in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al regolamento GDPR. Le misure devono garantire che siano trattati solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità, e garantisce che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica (Articolo 25 Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita);
- tiene il registro delle attività di trattamento (Articolo 30 Registri delle attività di trattamento) svolte sotto la propria responsabilità. Tale registro contiene le seguenti informazioni:
    - 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;
    - le finalità del trattamento;
    - una descrizione delle categorie di interessati e delle categorie di dati personali;
    - le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
    - ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
    - ove possibile una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1;

1

- se un tipo di trattamento a causa della tipologia, oggetto, contesto, finalità e strumenti tecnologici impiegati può presentare un rischio elevato, il titolare del trattamento, può effettuare una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi (Articolo 35 Valutazione d'impatto sulla protezione dei dati)

Il Titolare risponde della corretta applicazione della normativa in materia di protezione dei dati personali.

Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il Titolare del trattamento mette in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al regolamento UE 679/2016. Dette misure sono riesaminate e aggiornate qualora necessario.

Responsabili del trattamento

Responsabile al Trattamento

Il responsabile è il soggetto che esegue, dei trattamenti di dati personali per conto del titolare e ne risponde in solido in caso di inadempienze. Il titolare del trattamento viene designato dal titolare nella persona dell'ing. **Bruno Pennacchio nato il 07/08/1994 ad Aversa (CE) e domiciliato in Qualiano in Campania (NA) alla via Selva Piccola n. 30**

Nel rispetto di quanto previsto dall'art. 28, paragrafo 3, nello svolgimento dell'incarico, il responsabile del trattamento deve impegnarsi a:

a) trattare i dati personali soltanto per lo svolgimento delle finalità connesse all'esecuzione del servizio affidato e su istruzione documentata del titolare, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale; in tal caso, il Responsabile del trattamento informa il Titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;
b) garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
c) adottare tutte le misure tecniche e organizzative adeguate, come richieste dall'articolo 32 Regolamento UE 2016/679, per garantire un livello di sicurezza congruo rispetto al rischio derivante alla libertà ed all'onore degli interessati dal trattamento dei loro dati personali;
d) rispettare quanto previsto dall'art. 28, paragrafo 2 (autorizzazione scritta del Titolare del trattamento) e paragrafo 4 (contrattualizzazione dell'incarico) in caso di ricorso a un altro responsabile del trattamento;
e) assistere il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III del Regolamento UE 2016/679;
f) assistere il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 (sicurezza del trattamento, notifica data breach, eventuale DPIA, consultazione preventiva) del Regolamento UE 2016/679, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
g) non utilizzare i dati che gli sono stati comunicati dal titolare del trattamento per altre attività di trattamento, a non cederli e a non comunicarli a soggetti terzi, se non a seguito di espressa autorizzazione scritta del titolare stesso;
h) cancellare o restituire, a scelta del titolare, tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento o in caso di risoluzione del contratto con il titolare del trattamento, nonché a cancellare le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;

i) mettere a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi qui elencati;
j) consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato;
k) informare immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati;
l) verificare e controllare che nell'ambito della propria organizzazione il trattamento dei dati sia effettuato ai sensi e nei limiti degli artt. 5 (principi applicabili al trattamento) e 6 (liceità del trattamento) GDPR 679/2016 e coordinare tutte le attività e le operazioni di trattamento;
m) curare, ai sensi degli artt. 13 e 14 GDPR 679/2016, la messa a disposizione di eventuali ulteriori informative agli interessati che si rendessero necessarie, assicurando la predisposizione della modulistica e delle altre forme idonee di informazione;
n) collaborare con il titolare del trattamento per l'evasione delle richieste degli interessati e delle istanze dell'Autorità di Controllo competente;
o) sovrintendere ai processi di comunicazione, diffusione (se prevista da norme di legge), trasformazione, blocco, aggiornamento, rettificazione e integrazione dei dati.

Amministratori di sistema

Si definiscono amministratori di sistema quei soggetti preposti alla sicurezza, alla gestione e alla manutenzione delle banche dati, dei sistemi e delle infrastrutture informatiche di un'impresa, di un ente o organismo cui vengono associati anche gli amministratori di reti e gli amministratori di sistemi software complessi (figura già definita dall'art. 1, comma 1, lett. c) d.P.R. 318/1999 nella disciplina previgente al Codice Privacy) che, in ragione delle proprie mansioni, come ad esempio, attività tecniche quali il salvataggio dei dati (backup/recovery), l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e manutenzione hardware, possono avere il privilegio di accedere – accesso da considerarsi anche solo in via potenziale – ai dati personali trattati dal titolare.

Tuttavia, anche se il GDPR non menziona la figura di amministratore di sistema, lo stesso GDPR impone a carico del titolare e del responsabile del trattamento maggiore controllo e responsabilizzazione, secondo un'ottica di prevenzione del rischio in relazione ai dati personali, allora la designazione degli amministratori di sistema nel rispetto di quanto impartito dal Garante con il suo provvedimento *"Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema"* del 27 novembre 2008, in G.U. n. 300 del 24 dicembre 2008 appare tuttora essere conforme ai principi e alle disposizioni contenute nel Regolamento Europeo sulla protezione dei dati personali.

Autorizzati al trattamento

L'art. 2- quaterdecies del Decreto Legislativo n. 101 del 10 agosto 2018, che ha novellato il previgente Codice Privacy italiano, ha disposto che il Titolare o il Responsabile del trattamento possano prevedere, sotto la loro responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operino sotto la loro autorità.

In tal modo è possibile mantenere le funzioni ed i compiti assegnati a figure interne dell'organizzazione che potevano essere definiti, a seconda dei casi, responsabili o incaricati ai sensi del previgente codice in materia di protezione dei dati personali ma in contrasto con il regolamento europeo.

Peraltro, già nelle linee guida del Garante *(https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6807118)* si afferma che "le disposizioni del Codice in materia di incaricati del trattamento sono pienamente compatibili con la struttura e la filosofia del regolamento".

Ne consegue che quanto disposto all'art. 29 del GDPR possa concretizzarsi con l'individuazione dei soggetti autorizzati al trattamento dati all'interno dell'azienda, prima denominati "incaricati". È sottolineata l'importanza di fornire istruzioni a tali soggetti: a tal fine sono previsti percorsi di formazione adeguati a coloro

che sono coinvolti nel trattamento dati in azienda.

Ciascun dipendente è assegnato stabilmente, all'atto dell'assunzione o nel caso di cambiamento di mansione, presso una o più strutture organizzative presso cui sono trattati i dati e per ciascuna delle quali sono individuate le categorie di dati cui si può avere accesso e gli ambiti del trattamento.

Si è provveduto a formare tutti gli autorizzati al trattamento dei dati e a fornire loro le adeguate istruzioni da seguire per eseguire il trattamento in sicurezza.

Il titolare o il responsabile del trattamento svolge le operazioni di trattamento mediante la preposizione e l'ausilio di persone fisiche: si tratta dei soggetti autorizzati al trattamento (ai sensi dell'art. 29 GDPR).

Secondo la definizione riportata nel GDPR si tratta di *"chiunque agisca sotto l'autorità del titolare o del responsabile del trattamento, dovendo essere istruito con un atto scritto".*

Ogni persona che all'interno dell'organizzazione tratta dati personali si qualifica come autorizzato al trattamento dei dati

Gli autorizzati al trattamento ricevono idonee ed analitiche istruzioni, anche per gruppi omogenei di lavoro, sulle mansioni loro affidate e sugli adempimenti cui sono tenuti.

In caso di trattamento automatizzato di dati, per ogni addetto al trattamento viene indicato lo USER-ID assegnato.

Il tipo di trattamento effettuato da ogni singolo addetto al trattamento può essere differenziato.

Ciascun Autorizzato deve limitarsi a trattare dati personali in funzione di quanto strettamente necessario in relazione all'esercizio delle proprie mansioni ed in conformità con le indicazioni operative ricevute, sotto l'autorità diretta del Titolare.

In particolare, ad ogni addetto al trattamento può essere data, dal titolare del trattamento, la possibilità di:

- Inserire nuove informazioni nella banca di dati personali
- Accedere alle informazioni in visualizzazione e stampa
- Modificare le informazioni esistenti nella banca di dati personali
- Cancellare le informazioni esistenti nella banca di dati personali

Ad ogni autorizzato sono state comunicate le credenziali per l'autenticazione per l'accesso al sistema e le relative istruzioni di sicurezza (segretezza delle credenziali, blocco del computer in propria assenza temporanea durante una sessione di trattamento).

All'amministratore di sistema è affidato il compito di verificare ogni sei mesi le autorizzazioni di accesso ai dati oggetto del trattamento e di aggiornare l'elenco degli utenti autorizzati.

Gli autorizzati al trattamento possono essere sia soggetti interni all'organizzazione aziendale, sia soggetti esterni, che operano autonomamente oppure all'interno di una organizzazione.

L'elenco dei soggetti eventualmente nominati come responsabili è riportato nell'allegato 3. L'allegato viene aggiornato ogni qualvolta un soggetto nuovo debba essere inserito oppure rimosso

Principi privacy generali

Ambito di applicazione e scopo	La presente Policy si applica alla LEOMIND srl nelle attività di trattamento di dati personali nel corso dello svolgimento dell'attività di business. Lo scopo del documento è quello di disciplinare le attività di trattamento di dati personali, al fine di garantire la piena conformità alle disposizioni dettate dal Regolamento Europeo n. 2016/679 (GDPR)
Trattamento e finalità	Con riferimento ai dati personali, la LEOMIND s.r.l. tratta dati sensibili e personali forniti dai propri clienti diritte ed indiretti oltre ai dati trattati nello svolgimento dei rapporti di lavoro con i propri dipendenti. La LEOMIND s.r.l. nello svolgimento ed esecuzione dei contratti conclusi con i clienti, utilizza i dati personali solo per il raggiungimento delle finalità connesse (quali, ad es., esecuzione del contratto, adempimenti assistenziali, e sicurezza sul lavoro; attività di verifica, attività formative e di sviluppo, valutazione delle performance; utilizzo di dati personali, incluse immagini fotografiche e video). I dati personali degli interessati, sono trattati per le seguenti finalità: - Per gli scopi connessi all'attività della azienda e per l'esecuzione di contratti e/o obbligazioni di cui l'azienda è parte art. 6 comma 1 lett. b); - Adempiere agli obblighi derivanti da rapporti in essere, agli obblighi previsti dalla legge, da un regolamento, dalla normativa comunitaria o da un ordine dell'Autorità, tra cui per aspetti Contabili, Fiscali art. 6 comma 1 lett. c); - Esercitare il legittimo interesse del titolare del trattamento art. 6 comma 1 lett. f);

Interessati Ordinari	Gli interessati sono: - soci - membri di organi sociali - personale interno (diretto, somministrato) - tirocinanti – stagisti - personale di cooperative di lavoro - clienti persone fisiche - clienti soggetti giuridici - fornitori - referenti indicati dai clienti/fornitori stessi - enti e professionisti incaricati della prestazione di servizi (terze parti) - referenti di potenziali clienti che richiedano espressamente informazioni commerciali - nominativi derivanti a candidature spontanee di lavoro e/o ai fini di stage aziendali
Tipologia di dati	Dati conferiti spontaneamente e volontariamente dagli interessati sopra identificati, tra cui: - Dati comuni (dati identificativi, anagrafici, di fatturazione, di recapito e simili) - Alcune tipologie di dati particolari che rivelino le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale intesi a identificare in modo univoco una persona fisica, dati relativi alla salute della persona ai sensi dell'art. 9 GDPR - Dati provenienti dal sito web (automatici, forniti attraverso form di contatto)
Descrizione del sistema informatico interno	Il sistema informatico aziendale è riportato nel dettaglio nel documento allegato*:* ***- descrizione del sistema***
Profilazione degli autorizzati	Tutti gli autorizzati ad accedere ai dati sono dotati di codici per l'accesso ai dati. In funzione dell'incarico, saranno abilitati all'accesso con opportune credenziali identificative che ne determinano le relative autorizzazioni. In ogni caso l'accesso ai sistemi di elaborazione dati è consentito solo con codici e password che verranno modificate e sostituite ogni 3 mesi. I soggetti autorizzati all'accesso dei codici e delle password sono riportati nell'allegato B e l'autenticazione è definita con password.
Misure di sicurezza nel trattamento dei dati	La società LEOMIND srl adotta tecnologie sicure e ragionevoli precauzioni per proteggere i dati personali contro l'indebita divulgazione, alterazione o uso improprio. Le protezioni attivate si propongono, in particolare, di ridurre al minimo

	i rischi di distruzione e di perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta. Nell'ambito aziendale vengono condotte attività periodiche di analisi dei rischi per verificare l'aderenza agli standard di sicurezza definiti ed eventualmente adottare nuove misure di sicurezza a seguito di cambiamenti organizzativi ed innovazioni tecnologiche o cambiamenti nella tipologia dei dati raccolti. Le misure di sicurezza sono costantemente controllate e periodicamente verificate. Le misure di sicurezza sono riportate nel nell'allegato C
Assessment	Il Titolare effettua una periodica autovalutazione al fine di verificare che la presente Policy venga applicata e che tutte le persone si conformino ai presenti principi.
Responsabili del Trattamento	Le Terze Parti (fornitori, clienti, business partner, consulenti) che svolgono attività di qualsiasi tipo per l'offerta di beni e servizi di LEOMIND srl, in relazione alle quali effettuano operazioni di trattamento di dati personali per conto delle stesse, saranno responsabili personalmente per i dati che i terzi rilasceranno. La società LEOMIND srl, invece tratterà i dati che gli verranno forniti dai clienti diritte ed indiretti secondo quanto previsto nel presente modello. Il titolare per i dati in suo possesso diretti ed indiretti attribuisce particolare importanza alla protezione della riservatezza dei dati personali, sollecitando il contributo di tutte le parti per il raggiungimento di tale obiettivo.
Comunicazioni dei dati	La comunicazione dei dati personali conferiti può avvenire su richiesta degli stessi clienti dipendenti e collaboratori del Titolare, nella loro qualità di autorizzati al trattamento. I dati possono essere comunicati a soggetti terzi per adempiere ad obblighi di legge, in esecuzione di ordini provenienti da pubbliche autorità ovvero per fare valere o difendere un diritto in sede giudiziaria per necessità di business e per fini amministrativi interni, compreso il trattamento dati personali di clienti e dipendenti. I dati personali possono essere comunicati a soggetti terzi, in qualità di autonomi Titolari del trattamento o di Responsabili del trattamento, con il consenso degli Interessati, se richiesto per legge, e comunque previa adeguata informativa volta a specificare le finalità del trattamento.
Diffusione dei dati	La LEOMIND srl NON effettua diffusione dei dati.
Conservazione dei dati	**Candidati** I dati personali dei candidati non selezionati sono conservati per il periodo strettamente necessario al perseguimento delle finalità di selezione e assunzione del personale. In particolare, dopo **12 mesi** dall'inizio del trattamento, ossia dallo screening dei curricula, dovranno essere cancellati i dati dei candidati in relazione ai quali non vi sia stato alcun evento per l'intero periodo di conservazione previsto (e.g. modifica di dati personali, fissazione di un colloquio). **Dipendenti** I dati personali riguardanti i dipendenti vengono conservati per la gestione del rapporto di lavoro e per l'adempimento agli obblighi di legge. Gli stessi dati devono essere conservati successivamente al termine del contratto di lavoro al fine di dare corso a richieste di tutela di diritti ed interessi, ad eccezione di particolari trattamenti che possono presentare tempi più stringenti come i dati di formazione e valutazione. **Clienti** I dati personali riguardanti i clienti o comunicati da quest'ultimi nello svolgimento della propria attività saranno conservati nel termine pattuito dal contratto stesso. A discrezione del cliente, le tempistiche di conservazione a partire dalla chiusura del rapporto possono variare dalle intese contrattuali. In caso in cui non vi è alcuna clausola in merito, i termini di conservazione possono basarsi su: - l'art. 2220 Codice civile, ai sensi del quale le scritture contabili e i documenti a supporto devono essere conservati per 11 anni dalla data dell'ultima registrazione; **Fornitori** I dati personali riguardanti i fornitori devono essere conservati per la gestione del rapporto e per l'adempimento agli obblighi di legge. Gli stessi dati

	devono essere conservati **11 anni** successivamente al termine del contratto al fine di dare corso a richieste di tutela di diritti ed interessi. **Collaboratori** I dati personali riguardanti i collaboratori devono essere conservati per la gestione del rapporto di collaborazione e per l'adempimento agli obblighi di legge. Gli stessi dati devono essere conservati a tempo indeterminato successivamente al termine del contratto di collaborazione al fine di dare corso a richieste di tutela di diritti ed interessi. **Log Amministratori di sistema**

	I log di accesso ai sistemi informativi saranno conservati per un periodo di almeno 3/6 mesi al fine di consentire verifiche a posteriori, come consentito dal Provvedimento del Garante in materia (*punto 4. 5 del Provv. 27 novembre 2008*).
Registro dei Trattamenti	Per dimostrare che il Titolare del trattamento ottempera alle disposizioni del Regolamento europeo, deve essere compilato il Registro delle attività di trattamento effettuate sotto la sua responsabilità. La società LEOMIND S.r.l. in qualità di titolare del trattamento si è dotata di un unico Registro di Gruppo nel quale, sono riportati i singoli trattamenti individuati e mappati. Il Registro dei Trattamenti è parte integrante di un sistema di corretta gestione dei dati personali

Mappa delle tipologie dei trattamenti assegnati alle funzioni

In azienda vengono effettuati i seguenti trattamenti:

- trattamenti amministrativi e fiscali in ottemperanza di obblighi contabili, fiscali e contrattuali in accordo con le norme di legge;
- trattamenti sui dati personali ed in particolari dei clienti e dei dati forniti;
- trattamenti per la gestione commerciale di contratti;
- trattamenti su potenziali clienti;
- trattamenti per la gestione delle attività del titolare
- trattamenti per l'affidamento e la gestione del contenzioso e del recupero dei crediti.

Sigle tipologia interessati	Descrizione
CL	CLIENTI
POT-CL	POTENZIALI CLIENTI
F	FORNITORI
DIP	DIPENDENTI
CAND	CANDIDATI
DB-CL	DATA BASE CLIENTI
DB-POT-CL	DATA BASE POTENZIALI CLIENTI
DB-F	DATA BASE FORNITORI
DB_DIP	DATA BASE DIPENDENTI
Sigle tipologia dei trattamenti	**Descrizione**
COM-ID	COMUNI IDENTIFICATIVI
PART	DATI PARTICOLARI (art. 9 GDPR) 1. dati che rivelano l'origine razziale o etnica 2. dati che rivelano le opinioni politiche 3. dati che rivelano le convinzioni religiose 4. dati che rivelano l'appartenenza sindacale 5. dati biometrici 6. dati relativi alla salute 7. dati relativi alla vita/orientamento sessuale
GIU	GIUDIZIARI (art. 10 GDPR) 5. dati relativi a indagini penali in corso 6. dati relativi a condanne penali 7. dati relativi a carichi pendenti 8. dati relativi a casellario giudiziale

Struttura funzione aziendale	Tipologia interessati	Trattamenti e dati	Descrizione dei compiti e delle responsabilità della struttura
Area Acquisti e gestione fornitori	CL - POT CL - F - DB-F	Dati relativi economici e identificativi dei fornitori	Acquisizione e caricamento dati, consultazione e comunicazione a terzi

Fatturazione attiva	CL DB-CL	Dati relativi economici e identificativi dei clienti	Acquisizione e caricamento dati, consultazione e comunicazione a terzi
Area Operativa	CL F DB-CL DB_F	Dati inerenti a fornitori e clienti e del personale interno dipendente e in somministrazione	Gestione di consultazione dati e comunicazione a terzi
Gestione del personale	DIP DB-DIP	Dati inerenti alla operatività, economici, sullo stato di salute, dati che rivelano l'appartenenza sindacale, dati biometrici, dati relativi alla salute del personale interno	Gestione di consultazione dati e comunicazione a terzi
Paghe e contributi	DIP DB-DIP	Dati inerenti alla operatività, economici e del personale interno	Gestione di consultazione dati e comunicazione a terzi
Sicurezza sul lavoro	DIP	Dati identificativi e sulla sicurezza dei lavoratori	Gestione di consultazione dati e comunicazione a terzi
Sistemi informativi	DB-CL DB-F DIP	Dati inerenti ai programmi di utilizzo aziendale	Gestione tecnica operativa della base dati (salvataggi, ripristini, ecc.), manutenzione tecnica dei programmi
Gestione qualità	CL F	Dati inerenti alla qualità, operativi ed economici	Gestione tecnica operativa ed economica dei dati; Consultazione dei Dati

Analisi Dei Rischi e Sistema di Sicurezza

Il GDPR è finalizzato, ai sensi dell'art. 32, al presidio della sicurezza dei trattamenti di dati: *"tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio".*

La sicurezza può essere definita come *"l'insieme delle misure atte a garantire la disponibilità, l'integrità e la riservatezza delle informazioni gestite"* e dunque *"l'insieme di tutte le misure atte a difendere il sistema informativo dalle possibili minacce d'attacco"*.

Le principali attività che l'azienda ha attivato per effettuare, in sicurezza, i trattamenti dei dati riguardano:

- **Sicurezza Fisica:** la funzione svolta dalla sicurezza fisica è quella di predisporre tutti i mezzi e gli strumenti necessari per proteggere persone, cose e ambienti da eventuali rischi. Si suddivide in sicurezza dell'area preordinata ad evitare accessi fisici non autorizzati e sicurezza delle apparecchiature hardware preordinata alla protezione da manomissione o furti dell'hardware e comprende anche la manutenzione degli stessi;
- **Sicurezza Logica:** la funzione svolta dalla sicurezza logica è quella di proteggere i dati oggetto di trattamento, attraverso misure di sicurezza di carattere tecnologico (c.d. Information and Communication Technology). Rientrano in questa area i c.d. sistemi di sicurezza preordinati alla protezione di tutte le piattaforme dati presenti in azienda (in primis mediante controllo accessi); meccanismi di sicurezza preordinati alla creazione del modus operandi dei sistemi di sicurezza (cifratura, firma digitale, meccanismi per l'autenticazione ecc.);
- **Sicurezza Organizzativa:** la funzione svolta dalla sicurezza organizzativa è quella di prevedere regole e procedure finalizzate a disciplinare gli aspetti organizzativi del processo di sicurezza fisica e logica. In questa area rientrano tutte le prescrizioni riguardanti la definizione dei ruoli, la distribuzione dei compiti e delle responsabilità. Quindi a titolo esemplificativo rientrano in questa area tutte le procedure relative alla gestione delle contromisure di sicurezza logica, così come le procedure per la sicurezza della rete, le procedure riguardanti il personale, le procedure di aggiornamento dei software, le procedure di backup, le procedure di formazione degli incaricati e dei responsabili ecc.…

I rischi di perdita dei dati, anche accidentale, di accesso abusivo e di trattamento illecito o non consentito dei dati possono essere causati (a titolo meramente esemplificativo) da:

- malfunzionamenti di sistemi hardware e software, applicativi software e servizi;
- persone esterne all'organizzazione (hacker, spie, terroristi, vandali, ecc.);
- eventi naturali (inondazioni, incendi, terremoti, tempeste, ecc.);
- persone interne all'organizzazione;

L'approccio alla sicurezza avviene in una logica di prevenzione (ossia mediante l'utilizzo di metodologie e di strumenti di *risk management*) piuttosto che in una logica di gestione delle emergenze o di semplice controllo / vigilanza.

Le misure tecniche ed organizzative devono essere adottate mediante l'utilizzo di un **processo di autodeterminazione**, per cui occorre provvedere alla riduzione dei rischi, che possono interessare i dati personali oggetto di trattamento in seno all'azienda e che riguardano il sistema informativo nel suo complesso.

Il sistema di sicurezza aziendale si basa sui seguenti principi generali:

- tutte le informazioni (dati, documenti, archivi, …) devono essere protette e disponibili;
- al fine di garantire la riservatezza dei contenuti e delle informazioni, la sicurezza deve riguardare anche le reti di comunicazioni elettroniche dei dati;
- si deve procedere alla previsione di misure di sicurezza per la protezione delle aree e locali, in cui sono localizzati i server considerati "sensibili" per l'attività dell'azienda e gli archivi cartacei, monitorandone le caratteristiche tecniche e le misure di tutela dagli accessi non autorizzati;
- tutte le operazioni di trattamento dei dati, effettuate utilizzando strumenti connessi alla rete di comunicazione elettronica, devono essere oggetto di tracciabilità, garantendo il non ripudio delle operazioni svolte, dovendo utilizzare un sistema di autenticazione informatica, che consenta un controllo dell'identità di "chi sta facendo che cosa";
- devono essere predisposte misure tecniche ed organizzative di sicurezza per l'accesso ai locali, che ospitano i server e gli strumenti elettronici in dotazione alle postazioni di lavoro, favorendo possibilmente la localizzazione e l'ubicazione in unico luogo o in luoghi collegati, al fine di consentire una migliore gestione degli strumenti e della sicurezza attiva e passiva;
- ogni eventuale incidente o evento straordinario, che possa pregiudicare la sicurezza dei dati e dei sistemi, deve essere oggetto di analisi e di rapporto scritto;
- tutti i progetti per lo sviluppo di nuovi sistemi / servizi, aventi natura trasversale e che possano interessare il sistema informativo dell'azienda, devono essere avviati secondo le prescrizioni di cui all'art. 25 GDPR e gestiti secondo quanto riportato nel presente manuale;
- al pari, tutte le modifiche eventualmente apportate ai processi organizzativi devono essere documentate nel presente manuale o nei documenti del sistema di qualità aziendale.

Sono identificati, per ciascuna risorsa critica, i rischi per i quali devono essere adottate misure di sicurezza adeguate.

I singoli rischi sono stati raggruppati in termini di:

- **rischi per la <u>riservatezza</u> dei dati**: le informazioni devono essere accessibili ed utilizzate solo da persone autorizzate e per fini conformi agli obiettivi aziendali;
- **rischi per la <u>integrità</u> dei dati:** i dati devono essere esatti, aggiornati e corrispondenti alla realtà; essi, inoltre, devono essere protetti contro qualunque forma di alterazione non controllata;
- **rischi per la <u>disponibilità</u>**: l'accesso ai dati deve poter avvenire ogni qual volta ve ne sia necessità in conformità alle esigenze dei trattamenti;

A tal fine, per ciascun sistema di sicurezza aziendale, deve essere fornita la cosiddetta **garanzia "R.I.D."**, ossia "**Riservatezza** – **Integrità** – **Disponibilità"**:

- **Riservatezza**: divulgazione - accesso;
- **Integrità**: protezione contro alterazioni o danneggiamenti;
- **Disponibilità**: distruzione – indisponibilità - perdita.

Garanzia	Evento	Rischio inerente
Disponibilità	I dati sono critici per l'organizzazione	La perdita o non accessibilità ai dati può provocare il fermo dei processi primari
Disponibilità	Esiste il rischio di incendio	Può causare la distruzione dei dati o delle loro copie
Disponibilità	Esiste il rischio di inagibilità del locale	I dati possono essere temporaneamente non accessibili
Disponibilità	Esiste il rischio di impossibilità di accesso	I trattamenti effettuati mediante la piattaforma non sono operativi
Disponibilità	Non esiste piano di contingenza	Non conoscere come operare in caso di situazioni di emergenza
Disponibilità	Il piano di contingenza non viene periodicamente verificato	Impossibilità di verificare la competenza dei soggetti interessati e la fattibilità del piano medesimo
Disponibilità	Esiste il rischio di sovraccarico	Scarsa operatività, tempi di esecuzione dei trattamenti non più compatibili con le esigenze
Disponibilità	Esiste il rischio di danneggiamento accidentale	Fermo dei processi aziendali coinvolti per cause accidentali
Disponibilità	Esiste il rischio di danneggiamento doloso	Fermo dei processi aziendali coinvolti con specifico obiettivo di causare danni
Disponibilità	Esiste il rischio di furto	Fermo dei processi aziendali, necessità di reintegro
Disponibilità	Non esiste la documentazione del trattamento	Impossibilità di comportamenti operativi standard; impossibilità di impiego di personale occasionale
Disponibilità	La documentazione non è aggiornata	Errori e ritardi nell'esecuzione del trattamento
Integrità	Esiste il rischio di perdita o distruzione della documentazione	Necessità di reintegro
Integrità	Esiste il rischio di errori nella raccolta	Imprecisione, errore nei processi e nelle decisioni
Integrità	Esiste il rischio di danneggiamento accidentale	Necessità di reintegro, uso dei back up, perdita di informazione
Integrità	Esiste il rischio di danneggiamento doloso	Necessità di reintegro, uso dei back-up, perdita di informazione per obiettivi specifici non definiti a priori
Integrità	Esiste il rischio di trafugamento	Accertamento del fatto, danni imprevedibili per uso non noto
Integrità	Non esiste il sistema di autorizzazione	Identità e qualifica del personale non certa
Integrità	Esiste il rischio di presenza di virus	Danneggiamenti imprevedibili
Integrità	Esiste il rischio di intrusione da hackers	Danneggiamenti imprevedibili
Integrità	Il trattamento non mantiene un registro degli accessi al trattamento	Impossibilità di ricostruzione degli eventi per l'identificazione delle cause di eventuali danneggiamenti
Integrità	Il trattamento non mantiene un registro di audit degli accessi	Impossibilità di ricostruzione degli eventi per l'identificazione delle cause di eventuali danneggiamenti, e di ripristinare l'integrità.
Riservatezza	Esiste il rischio di diffusione incontrollata	Uso abusivo dei dati
Riservatezza	I dati non sono mantenuti in forma crittografata	Impossibilità di circoscrivere la leggibilità dei dati solo per trattamenti noti ed autorizzati
Riservatezza	Non esistono sistemi di allarme anti-intrusione	Impossibilità di impedire l'accesso ai soggetti non autorizzati
Riservatezza	Gli accessi non sono registrati	Impossibilità di ricostruzione degli eventi per l'identificazione delle cause di eventuali danneggiamenti
Riservatezza	L'accesso non è soggetto ad autorizzazione	Impossibilità di accertare le qualifiche e capacità tecniche
Riservatezza	Il sistema non limita il numero dei tentativi di accesso	Impossibilità di contenere eventuali tentativi di intrusione
Riservatezza	Il sistema non mantiene un registro di audit degli accessi	Impossibilità di ricostruzione degli eventi per l'identificazione delle cause di eventuali danneggiamenti. Impossibilità di ripristinare l'integrità.

Riservatezza	Il sistema non termina la sessione in caso di time-out	Impossibilità di contenimento delle possibilità di abuso delle autorizzazioni
Riservatezza	dati non sono trasmessi in rete in forma crittografata	Impossibilità di circoscrivere la leggibilità dei dati solo per destinazioni note ed autorizzate
Riservatezza	Il numero dei tentativi di accesso non è limitato	Impossibilità di contenimento del rischio di uso non autorizzato
Riservatezza	Esiste il rischio di trafugamento della documentazione	Impossibilità di contenimento del rischio di uso non autorizzato
Uso	Esiste il rischio di utilizzo improprio	Possibilità di svolgere funzioni non autorizzate sui dati
Uso	Esiste il rischio di accesso non autorizzato	Mancanza di strutture di blocco degli accessi
Uso	L'autorizzazione non limita l'orario di accesso	Impossibilità di contenimento del rischio di accesso non autorizzato
Uso	Esiste il rischio di intercettazione dei dati	Uso abusivo dei dati
Uso	Esiste il rischio di accesso non autorizzato	Uso abusivo dei dati e dei trattamenti
Uso	Non esiste il sistema di autorizzazione	Incertezza della qualifica e capacità di colui che effettua il trattamento
Uso	L'autorizzazione non limita l'orario di accesso	Impossibilità di contenere il rischio di accesso non autorizzato
Uso	Esiste il rischio di accesso non autorizzato	Danneggiamento e/o abuso della risorsa e dei dati eventualmente presenti
Uso	L'orario delle diverse funzioni eseguibili non è limitato	Impossibilità di contenimento dei rischi di uso abusivo; insufficiente pianificazione del processo

In particolare, l'analisi e la valutazione dei rischi sono effettuate mediante l'individuazione delle singole minacce e vulnerabilità, per le quali si è provveduto a determinare il peso del rischio in termini di probabilità (P) e di danno (D), valutati secondo i parametri (critico – alto – medio - basso) associati a ciascuna minaccia.

Tipologia di impatto: basso

Valore numerico assegnato: 1

Impatto per violazione RID: i dati non presentano particolari requisiti di riservatezza. I dati sono pubblici. I dati non presentano particolari requisiti di integrità. I dati gestiti non fanno parte di transazioni economiche, finanziarie o sanitarie. L'indisponibilità dei dati oltre i tempi stabiliti contrattualmente non comporta multe o penali rilevanti.

Tipologia di impatto: medio

Valore numerico assegnato: 2

Impatto per violazione RID: i dati devono essere riservati per ragioni di business (concorrenza sleale, danni all'immagine), ma un'eventuale loro diffusione non ha elevati impatti sul business dell'organizzazione, sul rispetto della normativa vigente o sull'immagine dell'organizzazione. I dati non sono oggetto di transazioni di tipo economico, finanziario o sanitarie con impatti sul business di un'impresa. La mancanza di integrità dei dati non ha elevati impatti sulle attività operative o sul rispetto della normativa vigente. L'indisponibilità dei dati oltre i tempi stabiliti contrattualmente comporta multe o penali non particolarmente rilevanti.

Tipologia di impatto: alto

Valore numerico assegnato: 3

Impatto per violazione RID: i dati devono essere riservati per ragioni di business (concorrenza sleale, danni all'immagine) e un'eventuale loro diffusione ha elevati impatti sul business dell'organizzazione, sul rispetto della normativa vigente o sull'immagine dell'organizzazione. I dati non sono oggetto di transazioni di tipo economico, finanziario o sanitarie con impatti sul business di un'impresa. La mancanza di integrità dei dati ha elevati impatti sulle attività operative o sul rispetto della normativa vigente. L'indisponibilità dei dati oltre i tempi stabiliti contrattualmente comporta multe o penali rilevanti.

Tipologia di Impatto: critico

Valore numerico assegnato: 4

Impatto per violazione RID: la diffusione delle informazioni ha elevati impatti sul business dell'organizzazione o sul rispetto della normativa vigente o sull'immagine dell'organizzazione tali da compromettere la sostenibilità dell'organizzazione. La mancanza di integrità delle informazioni ha elevati impatti sul business aziendale o sul rispetto della normativa vigente tali da compromettere la sostenibilità dell'organizzazione. L'indisponibilità dei dati oltre i tempi stabiliti contrattualmente comporta multe o penali che mettono in pericolo la sostenibilità economica e di immagine o hanno impatti sulla sicurezza delle persone fisiche.

Evento pregiudizievole		Livello rischio	Azione di salvaguardia
COMPORTAMENTO DEGLI OPERATORI	Mancanza di formazione	2	Le risorse hanno una formazione annuale pianificata
	Sottrazione di credenziali di autenticazione	4	Gestione delle credenziali di accesso personali
	Carenza di consapevolezza	2	Le risorse hanno una formazione annuale pianificata
	Comportamenti sleali o fraudolenti	3	Le risorse sono persone affidabili formate e responsabilizzate come da lettere di incarico
	Errore materiale accidentale	2	Non vi sono dati vulnerabili ad errori accidentali nell'utilizzo corrente del gestionale (in ogni caso viene fatto back up giornaliero)
	Disattenzione o incuria	3	Le risorse hanno una formazione annuale pianificata
AZIONE DEI TERZI	Furti di attrezzature	3	Locale dotato di sistema di allarme Backup dati
	Rapine	2	Non si maneggiano denaro in contante o preziosi
EVENTI RELATIVI AGLI STRUMENTI	Uso non autorizzato del software	3	Utilizzo credenziali di accesso personali
	Accessi esterni non autorizzati	3	Il rooter è collegato al firewall
	Malfunzionamento, indisponibilità o degrado degli strumenti	3	Hardware di qualità che non ha mai dato problemi. Sistemi ridondanti e ad alta affidabilità
	Intercettazione delle informazioni in rete	2	Il rooter è collegato al firewall
	Spamming o tecniche di sabotaggio	2	Antivirus aggiornato periodicamente in automatico, gestione delle patch
	Azione di virus informatici o di programmi suscettibili di recare danno	4	Antivirus aggiornato periodicamente in automatico, gestione delle patch
CONTESTO FISICO AMBIENTALE	Ingresso non autorizzato a locali/aree ad accesso ristretto	3	Reception sempre presidiata, impianto di videosorveglianza sempre in funzione, i visitatori si ricevono solo per appuntamento oppure attendono di essere accompagnati in apposita saletta visitatori
	Sottrazione di strumenti contenenti dati	2	Reception sempre presidiata, impianto di videosorveglianza sempre in funzione, vigilanza interna notturna

	Eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali…) nonché dolosi, accidentali o dovuti ad incuria	3	Piano di disaster recovery; back up dei dati in rete e possibilità di ripristino anche su altro sistema
	Guasto a sistemi complementari (impianto elettrico, climatizzazione...)	2	back up dei dati in rete e possibilità di ripristino anche su altro sistema
	Errori umani nella gestione della sicurezza fisica	2	Le risorse hanno una formazione annuale pianificata

Misure Di Sicurezza

In considerazione delle risorse critiche e dei rischi individuati, vengono descritte le misure di sicurezza Fisiche ed Organizzative adottate nelle diverse sedi operative.

Le misure sono tali da rispettare gli obblighi previsti dalla Legge.

Misure di sicurezza generali sede operativa Salsomaggiore Terme (PR)

Sistemi di protezione comuni a tutti gli uffici/aree operative				
Accesso in azienda	☒ Controllato	☐ Non controllato	☒ Esiste un registro d'accesso	
Sistema antincendio	☒ Esiste	☐ Non esiste	☒ Estintori	
Sistema d'allarme	☐ Non esiste	☐ Allarme locale	☒ Allarme centralizzato	
Sistema videosorveglianza	☒ SI ☐ NO	☒ Con registrazione 24/48	☐ Con registrazione oltre 48	
Guardianeria o sorveglianza	☒ SI ☐ NO		☒ portierato orario lavoro	

Misure di sicurezza di area

Ufficio/Area operativa	**RECEPTION / UFFICIO CUSTOMER CARE**		
Dotazioni e sistemi di protezione	☐ Armadi blindati	☐ Armadi ignifughi con serratura	☐ Armadi ignifughi senza serratura
	☒ Armadi con serratura	☒ Armadi senza serratura	☐ Cassaforte
	☒ Scaffalature	☐ Finestre con inferriate	☒ Finestre senza inferriate
	☒ Classificatori/Cassettiere con serratura	☐ Classificatori/Cassettiere senza serratura	☐ Rilevatori temperatura ☐ Rilevatori Incendio
Chiusura	☒ Con serratura	☐ Senza serratura	
Distruggidocumenti	☒ Non Esiste	☐ Esiste	
Trattamenti eseguiti	Banche dati commerciali Banca Dati degli utenti dei servizi o interessati durante lo svolgimento dei servizi Banche dati in formato digitale e/o informatico: DOCUMENTI SINGOLI PC e POSTA ELETTRONICA. Banche dati relative all'attività specifica aziendale.		
Ufficio/Area operativa	**UFFICI AMMINISTRAZIONE/PERSONALE/ACQUISTI**		
Dotazioni e sistemi di protezione	☐ Armadi blindati	☐ Armadi ignifughi con serratura	☐ Armadi ignifughi senza serratura
	☒ Armadi con serratura	☐ Armadi senza serratura	☐ Cassaforte
	☐ Scaffalature	☐ Finestre con inferriate	☒ Finestre senza inferriate
	☒ Classificatori/Cassettiere con serratura	☐ Classificatori/Cassettiere senza serratura	☐ Rilevatori temperatura ☐ Rilevatori Incendio
Chiusura	☒ Con serratura	☐ Senza serratura	
Distruggidocumenti	☒ Non Esiste	☐ esiste	
Trattamenti eseguiti	Banche dati Amministrativo-Contabili: BANCHE, CLIENTI, DIPENDENTI E PAGHE, CURRICULA, FORNITORI. Banca dati su: formazione e sicurezza Banche dati in formato digitale e/o informatico: DOCUMENTI SINGOLI PC e POSTA ELETTRONICA.		
Ufficio/Area operativa	**DIREZIONE OPERATIVA**		
Dotazioni e sistemi di protezione	☐ Armadi blindati	☐ Armadi ignifughi con serratura	☐ Armadi ignifughi senza serratura
	☒ Armadi con serratura	☒ Armadi senza serratura	☐ Cassaforte
	☐ Scaffalature	☐ Finestre con inferriate	☒ Finestre senza inferriate
	☒ Classificatori/Cassettiere con serratura	☐ Classificatori/Cassettiere senza serratura	☐ Rilevatori temperatura ☐ Rilevatori Incendio
Chiusura	☒ Con serratura	☐ Senza serratura	
Distruggidocumenti	☒ Esiste	☐ Non esiste	
Trattamenti eseguiti	Banche dati commerciali: MARKETING E COMMERCIALE. Banca Dati degli utenti dei servizi o interessati durante lo svolgimento dei servizi Banche dati in formato digitale e/o informatico: DOCUMENTI SINGOLI PC e POSTA ELETTRONICA. Banche dati relative all'attività specifica aziendale: COMMESSE DI PRODUZIONE e SISTEMI DI GESTIONE		
Ufficio/Area operativa	**SALA SERVER**		

Dotazioni e sistemi di protezione	☐ Armadi blindati	☐ Armadi ignifughi con serratura	☐ Armadi ignifughi senza serratura
	☒ Armadi con serratura	☒ Armadi senza serratura	☐ Cassaforte
	☒ Scaffalature	☐ Finestre con inferriate	☒ Finestre senza inferriate
	☒ Classificatori/Cassettiere con serratura	☐ Classificatori/Cassettiere senza serratura ☐	☒ Senza Rilevatori temperatura ☒ Senza Rilevatori Incendio
Chiusura	☒ Con serratura	☐ Senza serratura	
Distruggidocumenti	☒ Esiste	Non esiste	
Trattamenti eseguiti	Banche dati Amministrativo-Contabili: BANCHE, CLIENTI, DIPENDENTI E PAGHE, CURRICULA, FORNITORI. Banche dati commerciali: MARKETING E COMMERCIALE. Banca Dati degli utenti dei servizi o interessati durante lo svolgimento dei servizi Banca dati su: formazione e sicurezza Banche dati in formato digitale e/o informatico: DOCUMENTI SINGOLI PC e POSTA ELETTRONICA. Banche dati relative all'attività specifica aziendale: COMMESSE DI PRODUZIONE e SISTEMI DI GESTIONE		

- **La sede di** VIALE CAVOUR 78, SALSOMAGGIORE TERME (PR) 43039 **rappresenta il domicilio dell'azienda ovvero il luogo in cui vengono impartite le direttive. Il Core Buisness dell'azienda ossia ove si trovano gli uffici amministrativi e la sede operativa è in Salsomaggiore (PR).**

Elenco documenti

Per assicurare la protezione dei dati si allegano i seguenti documenti: