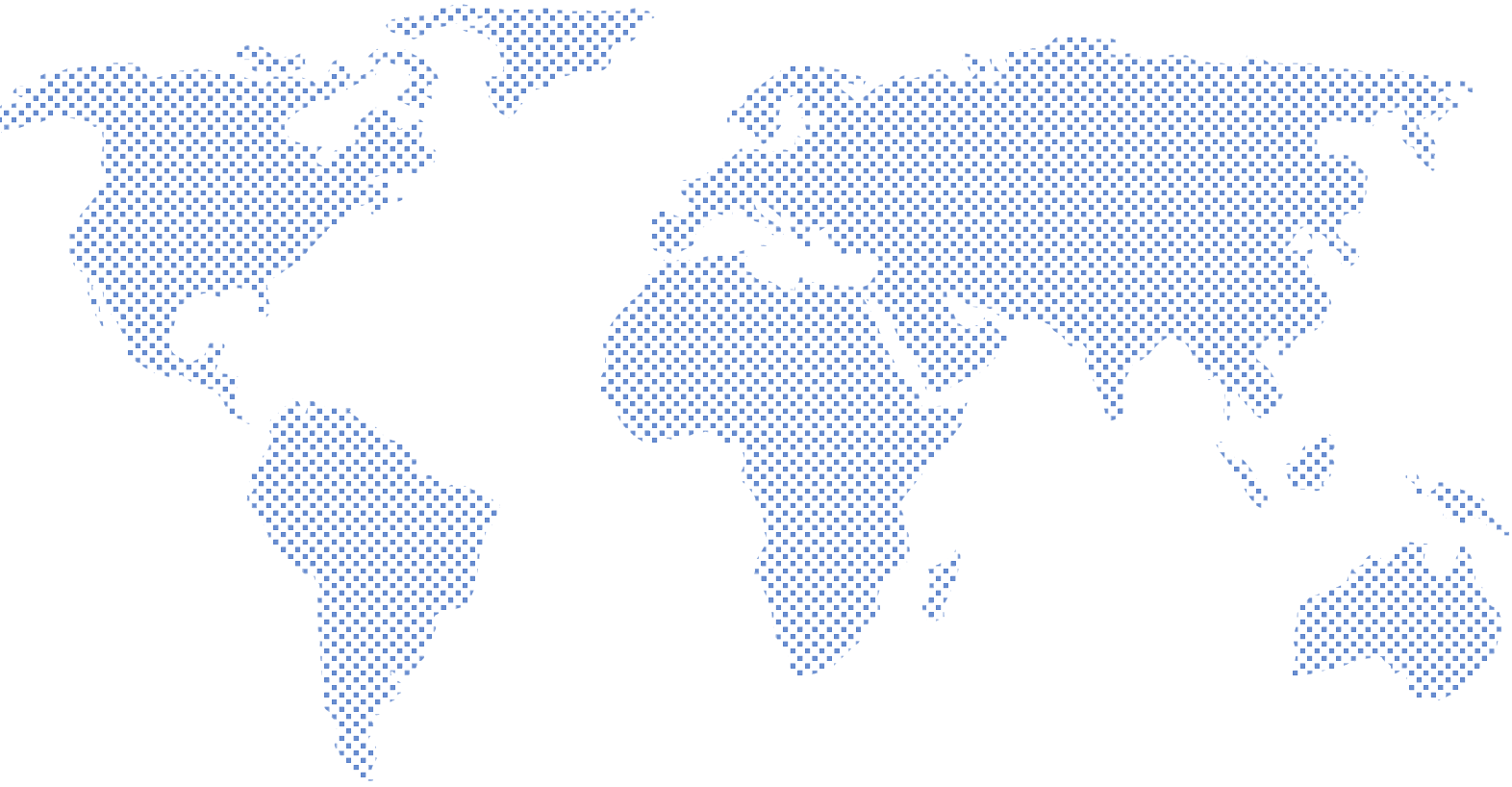
REGISTRO DELLE ATTIVITA' DI TRATTAMENTO

IN QUALITÀ' DI TITOLARE DEL TRATTAMENTO DATI

DOCUMENTO REDATTO AI SENSI DELL'ART. 30 COMMA 1 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



LA MORGIA ASSICURAZIONI SAS DI LA MORGIA DANIELE & C

A000568091 DEL 05 MARZO 2021

Sommario

1 Introduzione

LA MORGIA ASSICURAZIONI SAS DI LA MORGIA DANIELE & C ha un mandato agenziale di intermediazione assicurativa da parte di compagnie di assicurazione.
L'attività di distribuzione assicurativa consiste nel proporre e stipulare prodotti assicurativi delle compagnie mandanti, rispettando i regolamenti IVASS e la Direttiva 2016/679 EU in materia di distribuzione assicurativa, che impongono obbligatoriamente specifici trattamenti, anche al fine di valutare l'adeguatezza e/o la coerenza di un contratto o valutare il rischio di riciclaggio di denaro secondo quanto previsto dal Regolamento Ivass N. 44 del 12.02.2019.
Altre Normative obbligatorie sono:
D.Lgs. 209/05 Codice delle assicurazioni private, e relativi regolamenti IVASS
D.Lgs. 231/07 e Reg. Ivass n.44 02/19 in materia di antiriciclaggio e antiterrorismo
D.Lgs. 231/01 in materia di Responsabilità amministrativa delle persone giuridiche
D.Lgs. 81/08, in materia di salute e sicurezza sul lavoro
Direttiva Europea 2016/94/EU Insurance Distribution Directive di seguito "IDD".
A tal fine, l'agenzia opera in qualità di Titolare (art. 4 comma 7) del Trattamento dati, i cui Responsabili del Trattamento dati sono le compagnie mandanti. In tale ruolo, quindi, la ditta ha elaborato un *"Registro delle attività di trattamento in qualità di Titolare"* secondo quanto indicato dal regolamento Europeo 679/2016 all'art.30 e su esplicita richiesta delle compagnie mandanti. L'agenzia di assicurazione tratta anche altri dati in qualità di autonomo Titolare, anche per rispettare le normative obbligatorie in materia di contabilità fiscale e sul lavoro, il suddetto registro ne definisce lo svolgimento e ne assolve gli obblighi previsti dal Regolamento Europeo per la protezione dei dati.

Il presente documento si riferisce al solo trattamento dati svolto in qualità di Titolare (art. 4 comma 7 Gdpr).

2 Politica Aziendale

In qualità di Titolare (art. 4 comma 7 Gdpr) del trattamento, l'agente ritiene fondamentale, nello svolgimento delle proprie attività, il rispetto dei seguenti principi:

- Il trattamento dei dati degli interessati, in particolare dei propri dipendenti e dei propri clienti deve avvenire nel pieno rispetto dei loro diritti e conforme procedure ed istruzioni definite dal Reg. EU 679/2016.
- Il trattamento dei dati personali deve essere eseguito in pieno accordo al Regolamento Europeo sulla Privacy UE 2016/679 a tal fine al personale viene data adeguata formazione sugli adempimenti privacy e relativa informazione sulla presente politica e sulle istruzioni impartite tramite formazione attraverso piattaforma e-learning, intranet agenziale, dal contenuto visionabile in qualsiasi momento, oltre che da corsi in aula organizzati dalle Compagnie con le quali si è mandatari, i corsi sono obbligatori anche ai fini Ivass.

In particolare, si ritengono prioritarie le seguenti istruzioni:

- Le attività di marketing devono esser fatte solo con il consenso dell'interessato.
- È vietata la profilazione non autorizzata degli interessati.
- È vietato il trasferimento non autorizzato dal Garante della privacy di dati personali verso paesi terzi.
- Le misure di sicurezza definite devono essere attuate ed efficaci.

Al personale viene data adeguata formazione sugli adempimenti privacy e relativa informazione sulla presente politica e sulle istruzioni impartite.
La presente agenzia ha inoltre incaricato personale interno ed esterno al fine di verificare il rispetto di tali regole.

3 Ruoli

Responsabile del Trattamento : Compagnie Mandanti come indicato sui mandati in possesso dell'Agente. L'elenco completo e aggiornato è disponibile sul RUI

Titolare del trattamento:

Nome e Cognome/denomin. sociale:	Indirizzo:	Telefono, Fax:
LA MORGIA ASSICURAZIONI SAS DI LA MORGIA DANIELE & C	VIA ROMA, 53 - 24020 FIORANO AL SERIO (BG)	035 714808 - 035 721625
MAIL / PEC	**SITO INTERNET**	**Cellulare**
fiorano@lamorgiassicurazioni.it lamorgiaaasicurazioni@pec.it	/	/

L'agenzia si avvale, per il trattamento dei dati per finalità operative, di:

DIPENDENTI:

Si veda documento STRUTTURA ORGANIZZATIVA

Personale assunto con contratto di lavoro subordinato badato su contratti nazionali.

STAGISTI / TIROCINANTI:

Non presenti in struttura

Vincolati da contratto di stage / tirocinio.

COLLABORATORI:

Si veda documento STRUTTURA ORGANIZZATIVA

Personale esterno senza vincolo di subordinazione vincolati da un mandato.

Il documento *"Struttura Organizzativa"* nella sez. "*Organizzazione"* all'interno del fascicolo *"Sistema Gestione Compliance"* indica l'elenco completo del personale autorizzato al trattamento dati.

L'agenzia, per il trattamento dati per finalità amministrative, si avvale inoltre della collaborazione di:

- Professionisti: Consulenti del lavoro, Commercialisti e consulenti in organizzazione.

Tali figure sono nominate Responsabili Esterni del Trattamento dati, mediante apposita nomina concordata tra le parti, che fornisce anche istruzioni di base in materia di obblighi previsti, tale nomina si trova all'interno del fascicolo "Sistema Gestione Compliance" sez. "Privacy".

Tutti i rapporti ivi definiti contengono clausole di impegno alla riservatezza o hanno un adeguato obbligo legale di riservatezza e sono autorizzati al trattamento dati mediante Registro degli incarichi, contenuto nel documento *"Struttura Organizzativa"* all'interno del fascicolo *"Sistema Gestione Compliance"*.

Il personale ivi indicato è istruito direttamente dal titolare del trattamento dati mediante corsi di formazione dedicati su piattaforma e-learning o corsi in aula con formatori qualificati, valevoli e obbligatori anche ai fini IVASS.

Per le finalità indicate nel presente documento, l'agenzia non ha predisposto gli incarichi di:

- DPO (Data Protection Officer) ovvero Responsabile Protezione dei Dati

Non sono presenti accordi in tal senso.

- Responsabile della protezione dei dati:

Non sono soddisfatti i requisiti necessari previsti all'articolo 37 comma 1 del Regolamento Europeo 2016-679 che ne prevedono l'obbligo.

La presente agenzia non ha nominato sub-responsabili al trattamento dati.

4 Categorie di interessati e finalità

Categoria di interessati: CLIENTI

I clienti dell'agenzia di assicurazione sono sia persone giuridiche che fisiche.

Finalità 1A: Attività amministrativa

L'agenzia di assicurazione elabora dati dei clienti per adempiere agli obblighi di legge in materia di contabilità e fiscalità.

Finalità 1B: Analisi adeguatezza e/o coerenza assicurativa

L'agenzia di assicurazione acquisisce una serie di informazioni dei clienti al fine di verificare l'adeguatezza dei contratti offerti, secondo quanto previsto dai regolamenti obbligatori applicabili all'attività di distribuzione assicurativa (vedasi IDD e Reg. Ivass).

Finalità 1C: Marketing

L'agenzia di assicurazione acquisisce una serie di informazioni dei clienti o dei potenziali clienti al fine di individuare prodotti o servizi assicurativi da proporre ai propri clienti o a quelli potenziali.

Finalità 1D: Videosorveglianza

Se presente, la videosorveglianza nei locali agenziali riprende immagini dei clienti che accedono ai locali agenziali. La videosorveglianza è inserita per finalità di sicurezza. All'esterno le dovute tabelle atte ad indicarne la presenza.

Finalità 1E : Registrazione Telefonica,

"In caso di vendita a distanza" così come definita e disciplinata dalla norma di settore vigente, ivi comprese la registrazione di videochiamata, prima dell'eventuale registrazione viene inviata alla clientela apposita informativa privacy, si procede alla registrazione solo dopo l'approvazione di tale trattamento da parte del cliente stesso. La registrazione telefonica si rende necessaria laddove si configura la Vendita a distanza in accordo alla norma vigente di settore e disciplinata *dall'art. 83 del Regolamento Ivass n. 40 del 02 Agosto 2018*

Categoria di interessati: FORNITORI

I fornitori dell'agenzia di assicurazione forniscono prodotti e servizi necessari per il funzionamento amministrativo, quali carta, toner(sia il loro ritiro una volta esausti, sia la fornitura a nuovo), manutenzione dispositivi di sicurezza quali estintori.
Finalità 2A: Attività amministrative
Sono trattati i dati dei fornitori per svolgere gli adempimenti amministrativi in termini fiscali e di legge (fatturazione elettronica).

Categorie di interessati: DIPENDENTI E COLLABORATORI

L'agenzia di assicurazione acquisisce una serie di dati dei dipendenti (ove presenti) e dei collaboratori al fine di valutare la correttezza dell'attività di distribuzione assicurativa e alle attività amministrative, in particolare la formazione obbligatoria. Tali informazioni sono poi gestite dalle Compagnie mandanti per svolgere i controlli a cui sono obbligati secondo i regolamenti IVASS tra i quali Reg 40 del 02.agosto 2018e e la Direttiva 2016/97/EU .

Finalità 3A: Ricerca e selezione del personale
Sono trattati dati di potenziali dipendenti e collaboratori al fine di instaurare rapporti di lavoro.

Finalità 3B: Attività amministrative
Svolgimento di adempimenti fiscali, contabili e in materia del lavoro, secondo le norme e le leggi vigenti.
Svolgimento attività previste da obblighi di legge in materia di distribuzione assicurativa secondo i Regolamenti Ivass e la direttiva Europea in materia di distribuzione IDD.

Finalità 3C: Supporto al Marketing
Diffusione alla clientela, anche tramite sito internet, social Network, app di messaggistica crittografata, conformi alla cookie policy e privacy policy richiesta dal GDPR, atte a fornire informazioni per facilitarne la comunicazione con i clienti stessi.

Finalità 3D: Videosorveglianza
Qualora presente, l'utilizzo di sistemi di videosorveglianza è svolto per finalità di sicurezza nei locali agenziali.

5 Categorie di dati personali

Categorie di interessati	Finalità trattamento	Dati personali	Categorie dei dati (1)		
			I	S	G
CLIENTI	1A - Attività amministrativa	Identificativi	X		
	1B - Analisi adeguatezza assicurativa	Identificativi Prodotti assicurativi acquistati Dati idonei a valutare adeguatezza dei contratti offerti	X	X	
	1C -Marketing Promozione di prodotti e servizi assicurativi	Identificativi quali telefono, e-mail, social network, app. messagistica crittografata	X		
	1D- Videosorveglianza	Identificativi, quali immagini	X		
	1E- Registrazione Telefonica	Dati descritti in 1B,1C e Identificativi, quali immagini	X		
FORNITORI	2A - Attività amministrativa	Identificativi	X		
DIPENDENTI E COLLABORATORI	3A - Ricerca e selezione del personale	Identificativi e sensibili	X	X	
	3B - Attività amministrative	Identificativi Sensibili, in materia di appartenenza a sindacati Giudiziari, contenuti nel casellario giudiziale	X	X	X
	3C - Supporto all'attività di marketing agenziale	Identificativi	X		
	3D - Videosorveglianza locali	Identificativi, quali immagini	X		

1. Legenda: I = dato identificativo S = dato sensibile G = dato giudiziario

6 Categorie di destinatari

Categorie di interessati	Finalità trattamento	Categorie di destinatari
CLIENTI	1A - Attività amministrativa	Commercialista
	1B - Analisi adeguatezza assicurativa	Compagnie di assicurazione Altri intermediari assicurativi
	1C -Marketing Promozione di prodotti e servizi assicurativi	Altri intermediari assicurativi
	1D- Videosorveglianza	Ufficiali di Pubblica Sicurezza
	1E Registrazione Telefonica	Autorità di Vigilanza del Settore Assicurativo, Impresa di Assicurazione, Autorità Giudiziaria
FORNITORI	2A - Attività amministrativa	Commercialista
DIPENDENTI E COLLABORATORI	3A - Ricerca e selezione del personale	
	3B - Attività amministrative	Consulente del lavoro Consulente Organizzazione
	3C - Supporto all'attività di marketing agenziale	
	3D - Videosorveglianza locali	Ufficiali di Pubblica Sicurezza

Nessun dato è comunicato a destinatari di paesi terzi od organizzazioni internazionali.

7 Termini ultimi di cancellazione

Categorie di interessati	Finalità trattamento	Termine ultimo di cancellazione
CLIENTI	1A - Attività amministrativa	10 anni secondo leggi fiscali
	1B - Analisi adeguatezza assicurativa	10 anni per difesa in giudizio su attività professionale 5 anni di conservazione obbligatoria in materia Ivass
	1C -Marketing Promozione di prodotti e servizi assicurativi	Immediatamente dopo revoca del consenso
	1D- Videosorveglianza	24 ore
	1E Registrazione Telefonica	Secondo i termini di conservazione previsti dalle norme vigenti, ovvero in caso di contratti Ramo vita 10 anni
FORNITORI	2 A - Attività amministrativa	10 anni secondo leggi fiscali
DIPENDENTI E COLLABORATORI	3A - Ricerca e selezione del personale	6 mesi
	3B - Attività amministrative	10 anni secondo leggi fiscali
	3C - Supporto all'attività di marketing agenziale	Alla cessazione del rapporto di lavoro
	3D - Videosorveglianza locali	24 ore

8 Misure di sicurezza tecniche ed organizzative

Di seguito sono riepilogate le misure tecniche ed organizzative messe in atto per garantire un corretto trattamento dei dati degli interessati:

Categorie di interessati	Finalità trattamento	Misure tecniche ed organizzative
CLIENTI	1A - Attività amministrativa	Incaricato Responsabile Esterno Commercialista Attuate misure minime di sicurezza previste al punto 11 del presente Registro
	1B - Analisi adeguatezza assicurativa	Attuate misure minime di sicurezza previste al punto 11 del presente Registro Elaborata ISTRUZIONE **01**
	1C -Marketing Promozione di prodotti e servizi assicurativi	Elaborata ISTRUZIONE **02**
	1D- Videosorveglianza	Elaborata ISTRUZIONE **03**
	1E - Registrazione Telefonica	Elaborata ISTRUZIONE **08**
FORNITORI	2A - Attività amministrativa	Incaricato Responsabile Esterno Commercialista Attuate misure minime di sicurezza previste al punto 11 del presente Registro
DIPENDENTI E COLLABORATORI	3A - Ricerca e selezione del personale	Elaborata ISTRUZIONE **04**
	3B - Attività amministrative	Incaricati Responsabile Esterno Consulente del Lavoro e Consulente Organizzazione Attuate misure minime di sicurezza previste al punto 11 del presente Registro
	3C - Supporto all'attività di marketing agenziale	Elaborata ISTRUZIONE **02**
	3D - Videosorveglianza locali	Elaborata ISTRUZIONE **03**

Altre misure tecniche ed organizzative attuate:

Istruzione 5 - gestione delle modifiche ai mezzi di trattamento
Istruzione 6 - gestione delle richieste degli interessati
Istruzione 7 - segnalazione violazioni di privacy

Istruzione 01 - Distribuzione assicurativa

L'attività primaria di distribuzione assicurativa deve essere condotta secondo le istruzioni impartite dalla Compagnia, che assume il ruolo di Titolare del trattamento dati per la parte di suo interesse a riguardo all'interno della distribuzione dei prodotti assicurativi.

Tutti i dipendenti e collaboratori che svolgono l'attività di intermediazione assicurativa, devono procedere a informare i clienti del tratta mento dati da parte della suddetta agenzia in qualità di titolare del trattamento dei dati (art. 4 comma 7 Gdpr) e far firmare il consenso al trattamento per la finalità di intermediazione assicurativa e marketing nell'informativa privacy – **modello esemplificativo in sez. "Privacy" all'interno del fascicolo "Sistema Gestione Compliance"**

La scheda deve essere archiviata in apposito raccoglitore, separato da quello delle compagnie, preferibilmente in ordine per data.
Deve essere inoltre fleggato su tale sistema informatico l'avvenuta acquisizione del consenso.

Istruzione 02 - Svolgimento attività di Marketing

Le attività di promozione commerciale di prodotti assicurativi devono avvenire nel pieno rispetto delle istruzioni indicate nei relativi corsi di formazione resi disponibili su piattaforma e-learning dalle Compagnie di Assicurazione mandanti con relativo rilascio di attestato di formazione e partecipazione certificato.
In particolare:

- È fatto divieto di contattare un interessato senza preventivo consenso per l'attività di marketing.
- È fatto divieto di usare dati sensibili per attività di marketing e profilazione.
- È fatto divieto svolgere profilazione dei clienti.
- È fatto divieto di trattare il dato per finalità diverse dalla sua autorizzazione e acquisizione o laddove non sia strettamente necessario

Marketing tramite e-mail/fax:

E-mail e fax devono riportare la seguente dicitura:

Attenzione: Questo messaggio è destinato unicamente alla persona o al soggetto ai quali è indirizzato e può contenere informazioni riservate e/o coperte da segreto professionale, la cui divulgazione è proibita. Qualora non siate i destinatari designati non dovrete leggere, utilizzare, diffondere o copiare le informazioni trasmesse (Regolamento UE 679/16). Nel caso aveste ricevuto questo messaggio per errore, vogliate cortesemente contattare il mittente e cancellare il materiale dai vostri computer.

Marketing su social network:
Si ricorda che vige anche per questa modalità commerciale l'obbligo di comunicazione dell'informativa e richiesta di consenso PRIMA di svolgere promozione commerciale.

Marketing tramite siti internet:
Devono essere rispettate le normative in materia di cookies nella pagina iniziale, come richiesto dalla norma vigente e su indicazioni del Garante della Privacy.
Se presenti form di richiesta informazioni, deve essere fornita adeguata informativa privacy.
Se le attività di marketing, in particolare dal sito internet, prevedono l'utilizzo di dati personali dei collaboratori, quali immagini e numero di cellulare o e-mail, deve essere loro fornita
adeguata informativa secondo quanto previsto dal documento nel fascicolo "*Sistema Gestione Compliance"* nella sez. *"Fascicoli Personali"*.
Campagne di marketing: È preferibile usare sistemi di CRM per la tracciabilità delle campagne di marketing, identificando le attività svolte per ogni interessato.

Per agevolare le richieste di opposizione / revoca al trattamento dati, tutte le comunicazioni commerciali devono riportare l'indirizzo e-mail al quale riferirsi per esercitare tale diritto.

Istruzione 03 - Inserimento Videosorveglianza in agenzia

Per attivare rimpianto videosorveglianza è necessario:

- Predisporre le informative ai dipendenti sull'intenzione di installare un impianto di videosorveglianza (presente in sez. “Fascicoli Personali” all’interno di “Sistema Gestione Compliance”)
  Incaricare un Designato all'accesso dei dati di videosorveglianza (presente in sez. “Fascicoli Personali” all’interno di “Sistema Gestione Compliance”)
- Predisporre la domanda all'ispettorato del lavoro
- Predisporre la comunicazione ai dipendenti dell'attivazione dell'impianto di videosorveglianza (presente in sez. “Fascicoli Personali” all’interno di “Sistema Gestione Compliance”)

Senza autorizzazione dell'ispettorato del lavoro le telecamere di videosorveglianza NON possono essere attivate.
Tutte le aree sottoposte a videosorveglianza devono poi essere adeguatamente segnalate mediante cartelli conformi agli obblighi di legge.

Istruzione 04 - Gestione del personale

Ricerca personale

L'addetto/a amministrazione riceve i curriculum dei candidati in formato cartaceo o elettronico.
È necessario creare una cartella informatica accessibile in forma riservata in cui salvare i curriculum ricevuti.
I curriculum cartacei sono scansionati e inseriti nella cartella informatica.
Se necessario conservare i curriculum cartacei, questi sono tenuti in cartellina indicante solo la dicitura "Curriculum". La cartellina, qualora non presidiata dall'addetto amministrazione, deve essere tenuta in archivio chiuso a chiave.
I curriculum devono indicare l'autorizzazione al trattamento dati, altrimenti devono essere immediatamente cestinati.
I curriculum sono conservati per un tempo massimo di sei mesi, oltre il quale devono essere distrutti (cestinati se cartacei, cancellati se informatici).
Nel caso in cui il sito internet preveda forme di contatto per invio curriculum, deve essere fornita adeguata informativa.

Assunzione personale

In fase assuntiva, l'addetto/a amministrazione fornisce l'informativa privacy al dipendente/collaboratore e, se necessario, richiede il consenso per il trattamento dati per finalità specifiche:

- Videosorveglianza (vedi istruzione 03)
- Marketing su siti internet (vedi istruzione 02)

Qualora presente viene inoltre consegnato il Regolamento Aziendale**,** una cui copia deve essere firmata per presa visione ed accettazione.
Qualora il dipendente/collaboratore non avesse svolto adeguati corsi di formazione in materia di privacy, l'addetto/a amministrazione procede a richiedergli tali adempimenti prima di iniziare a svolgere il trattamento dei dati.
La documentazione creata viene archiviata in apposito fascicolo per persona, conservato in archivio protetto dall’addetto/a amministrazione.

Conclusione rapporto di collaborazione

In fare di cessazione del rapporto di collaborazione:
- Cancellare tutti i dati di marketing (dal sito internet, in brochure)
- Prendere cartellina persona e posizionarla nell'archivio morto, prevedendone la distruzione

Istruzione 5 - Gestione modifiche ai mezzi di trattamento

In sede di elaborazione del presente documento, il Consulente Privacy ha identificato tutti i mezzi che sono utilizzati per trattare i dati, sia con sistemi automatizzati che non.
L'agenzia provvederà a consultare il Consulente Privacy prima di intervenire sulla modifica dei mezzi, al fine di valutarne i rischi ed adottare le necessarie misure di protezione.
Qualora i dati coinvolgano i dipendenti, è necessario richiedere una loro consultazione.

Istruzione 6 - Gestione richieste degli interessati

Gli interessati possono precedere alle seguenti richieste:

RICHIESTA	AZIONE
Comunicare ai propri destinatari rettifiche o cancellazioni richieste	Mandare e-mail ai destinatari, informandoli delle rettifiche e delle cancellazioni da effettuarsi.
Accesso ai dati Il cliente può richiedere se e quali dati sono trattati.	Mandare una lettera o e-mail, indicando: - se è in corso o meno un trattamento dei dati a lui riferiti. - L'informativa privacy, indicante le finalità. Qualora richiesto, deve essere fornita copia della scheda dati del cliente, o accesso alla scheda informatica, in collaborazione con l'assistenza software, riportante tutti i dati trattati.
Richiesta di rettifica L'interessato richiede la rettifica di alcuni dati	Rettificare il data base e confermare per iscritto al contraente l'avvenuta rettifica
Richiesta di cancellazione	Distruggere la scheda cliente cartacea e cancellare la scheda informatica qualora presente, comunicando poi al contraente l'avvenuta cancellazione.
Richiesta di portabilità	Fornire i dati richiesti all'interessato e procedere alla loro cancellazione.
Opposizione al trattamento	L'opposizione al trattamento dati per le attività di intermediazione assicurativa non è accettata, essendo un legittimo interesse del professionista assicurativo. L'opposizione al trattamento dati per finalità di marketing deve essere registrata sulla scheda cliente e sul relativo sistema informatico.

Spetta direttamente all'agente, in qualità di Titolare del trattamento (art. 4 comma 7 Gdpr), rispondere in forma scritta alle richieste esercizio dei diritti dei dipendenti e collaboratori quali interessati al trattamento dei propri dati.
Qualora il contraente eserciti i suoi diritti, richiedendo ad esempio informazioni su quali dati sono posseduti, è compito di tutta la rete distributiva diretta inoltrare tale richiesta all'agente senza indebito ritardo.
Quest'ultimo dovrà poi rispondere in forma scritta al contraente entro trenta giorni, anche in formato elettronico.

Istruzione 7 - Segnalazione violazioni privacy

Chiunque ravvisi una violazione della privacy sui dati personali degli interessati, dipendenti, collaboratori e interessati deve segnalarlo alla struttura preposta al controllo interno, di:
LA MORGIA ASSICURAZIONI SAS DI LA MORGIA DANIELE & C
all'indirizzo pec: lamorgiaaasicurazioni@pec.it
Questi, provvederà immediatamente a segnalare la violazione secondo quanto previsto dall'art. 33 del Reg. 679/2016.

Istruzione 8 – Registrazione Telefonica

Preliminare

Prima di procedere alla registrazione telefonica, sarà necessario informare il cliente degli obblighi normativi vigenti in ambito di vendita a distanza, successivamente alla trasmissione di apposita informativa e consenso da parte di quest'ultimo si potrà procedere con al suddetta registrazione.

Archiviazione, Utilizzo e Backup

Terminata la procedura il file contenente la registrazione telefonica, sarà debitamente conservato in supporto digitale quale hard-disk esterno, del quale dovrà essere fatto backup periodo (settimanale). La conservazione di tale supporto e il relativo utilizzo è riservato al Titolare del trattamento e/o ai soggetti da questi autorizzati al trattamento dati. Il supporto è custodito in luogo sicuro al fine di evitarne la sottrazione o l'utilizzo di qualsiasi tipo a soggetti terzi non autorizzati.

Conservazione

I File contenenti le registrazioni telefoniche saranno conservati e custoditi per tutto il tempo previsto dalle vigenti norme di settore e successive modificazioni e integrazioni ovvero, 10 anni per le registrazioni telefoniche inerenti i contratti del Ramo Vita.

---

10 Valutazione d'impatto sulla protezione dei dati

In questa sezione sono descritti i principali eventi potenzialmente dannosi per la sicurezza dei dati, e sono valutate le possibili conseguenze e la gravità in relazione al contesto fisico-ambientale di riferimento e agli strumenti elettronici utilizzati.

Tabella valutazione rischio
Al fine di valutare ogni singolo rischio sarà rappresentato un modello matematico, nel quale gli effetti del rischio stesso dipendono dai seguenti fattori.
P = probabilità o frequenza del verificarsi dell'evento rischioso
G = gravità della conseguenza, ossia dell'entità del danno provocato dal verificarsi dell'evento dannoso secondo la seguente funzione:

RISCHIO = P x G

	PROBABILITÀ'		
	BASSA	MEDIA	ALTA
GRAVITA'			
BASSA	B	B	M
MEDIA	B	M	A
ALTA	M	A	A

Qualora il rischio sia ALTO, è obbligatorio definire adeguate azioni di mitigazione.
Qualora il rischio sia MEDIO, è consigliabile adottare azioni di mitigazione.

SCHEDA 1A	CATEGORIA INTERESSATI: CLIENTI			
Finalità del trattamento	GESTIONE AMMINISTRATIVA			
Adempimenti contabili e fiscali.				
Dati trattati:	Identificativi e sensibili			
Fonte:	Clienti			
Destinatari:	Commercialista			
Archivi:	Sistema Informatico di proprietà del commercialista			
Durata conservazione:	Secondo obblighi di legge in materia fiscale (10 anni)			
Liceità del trattamento	11 trattamento e necessario per adempiere ad un obbligo legale al quale è soggetto il titolare del trattamento *(art 6 comma 1 lettera C Req. UE 679/16)*			
VALUTAZIONE D'IMPATTO				
Pericolo	Misure attuate	G	P	R
Distruzione	Protezione sistemi a cura del commercialista	B	B	B
Perdita	Protezione sistemi a cura del commercialista	B	B	B
Modifica	Protezione sistemi a cura del commercialista	B	B	B
Divulgazione non autorizzata	Protezione sistemi a cura del commercialista	**B**	B	B
Accesso accidentale o non autorizzato	Protezione sistemi a cura del commercialista	B	B	B

SCHEDA 1B	CATEGORIA INTERESSATI: CLIENTI			
Finalità del trattamento	GESTIONE ASSICURATIVA			
Per valutare le esigenze assicurative e adempiere ad obblighi di legge in materia assicurativa, come valutare l'adeguatezza de! contratto, l'agente acquisisce copie di documenti dell'interessato contenenti anche dati personali particolari quali dati relativi allo stato di salute.				
Dati trattati:	Identificativi (nome, cognome), ma anche informazioni sulla posizione assicurativa dell'interessato, anche sensibili.			
Fonte:	I dati sono fomiti dagli interessati in fase di attività precontrattuale o contrattuale assicurativa			
Destinatari:	Altre compagnie di assicurazione e altri intermediari assicurativi			
Archivi:	Schedario Cartaceo/software			
Durata conservazione:	10 anni per la difesa in giudizio per l'esercizio dell'attività professionale			
Liceità de! trattamento	il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento (valutazione adeguatezza contrattuale, valutazione esigenze assicurative) furi. 6 *comma 1, lettera c) Reg. UE 679/161 nonché* per il perseguimento del legittimo interesse del titolare del trattamento ad esercitare la professione di agente di assicurazione (art. 6 *comma 1, lette f) Reg. UE 679/16)*			
VALUTAZIONE D'IMPATTO - supporti cartacei				
Pericolo	Misure attuate	G	P	R
Distruzione	Archivi in armadi protetti da incendi e calamità	M	B	B
Perdita	Archivi protetti	B	B	B
Modifica	Documenti cartacei non modificabili	B	B	B
Divulgazione non autorizzata	Documenti in archivio protetto.	B	B	B
Accesso accidentale o non autorizzato	Documenti posizionati su armadi segregati	B	B	B
VALUTAZIONE D'IMPATTO - supporti informatici				

Pencolo	Misure attuate	G	P	R
Distruzione	Eseguito Back up secondo paragrafo 11 Server protetto da incendio	B	B	B
Perdita	Eseguito Back up secondo paragrafo 11 Server protetto da incendio	B	B	B
Modifica	Archivi informatici ad accesso	B	B	B
Divulgazione non autorizzata	Misure minime applicate (firewall,	B	B	B
Accesso accidentale o non autorizzato	PC protetti da password di ingresso	B	B	B

SCHEDA 1C	CATEGORIA INTERESSATI: CLIENTI
Finalità del trattamento	MARKETING
Per proporre prodotti e servizi ai clienti.	
Dati trattati:	Identificativi (nome, cognome).
Fonte:	I dati sono fomiti dagli interessati in fase di attività precontrattuale o contrattuale
Destinatari:	Altre compagnie di assicurazione e altri intermediari assicurativi
Archivi:	Schedario Cartaceo/software
Durata conservazione:	Fino a revoca del consenso
Liceità del trattamento	il trattamento dei dati è lecito in seguito al consenso dell'interessato 'art. 6 comma 1. lette a) Reg. UE 679/16)

VALUTAZIONE D'IMPATTO - supporti cartacei

Pericolo	Misure attuate	G	P	R
Distruzione	Archivi in armadi protetti da incendi e calamità	M	B	B
Perdita	Archivi protetti	B	B	B
Modifica	Documenti cartacei non modificabili	B	B	B
Divulgazione non autorizzata	Documenti in archivio protetto.	B	B	B
Accesso accidentale o non autorizzato	Documenti posizionati su armadi segregati	B	B	B

VALUTAZIONE D'IMPATTO - supporti informatici

Pericolo	Misure attuate	G	P	R
Distruzione	Eseguito Back up secondo paragrafo 11 Server protetto da incendio	B	B	B
Perdita	Eseguito Back up secondo paragrafo 11 Server protetto da incendio	B	B	B
Modifica	Archivi informatici ad accesso	B	B	B
Divulgazione non autorizzata	Misure minime applicate (firewall, antivirus) Informative su e-mail presenti	B	B	B
Accesso accidentale u non autorizzato	PC protetti da password di ingresso	B	B	B

SCHEDA 1D	CATEGORIA INTERESSATI: CLIENTI
Finalità del trattamento	VIDEOSORVEGLIANZA
Ripresa e conservazione immagini di videosorveglianza per finalità di sicurezza locali.	
Dati trattati:	Immagini dei clienti
Fonte:	Telecamere di videosorveglianza
Destinatari:	Ufficiali di Pubblica Sicurezza
Archivi:	hard disk dedicato
Durata conservazione:	24 ore
Liceità del trattamento	il trattamento dei dati è lecito in seguito al consenso dell'interessato 'art. 6 comma 1. lette a) Reg. UE 679/16)

VALUTAZIONE DTMPATTO

Pencolo	Misure attuate	G	P	R
Distruzione	Hard disk protetto da incendio	B	B	B
Perdita	Hard disk protetto	B	B	B
Modifica	Accesso hard disk solo con chiave	B	B	B
Divulgazione non autorizzata	Accesso hard disk solo a personale designato	B	B	B

Accesso accidentale o non autorizzato	Accesso hard disk solo a personale	B	B	B

SCHEDA 2A	CATEGORIA INTERESSATI: FORNITORI
Finalità del trattamento	ACQUISTO PRODOTTI E SERVIZI

Dati trattati per finalità amministrative (emissione ordini di acquisto, fatturazione).
1 dati sono inviati via posta od e-mail ai fornitori ed inseriti su sistema informatico dedicato,
1 fornitori sono entità giuridiche e quindi non rientranti nella normativa privacy.

Dati trattati:	Dati societari, e-mail, telefono, pec Dati personali dei dipendenti del fornitore
Fonte:	Fomiti direttamente dai fornitori di prodotti e servizi
Destinatari:	Commercialista
Archivi:	Sistema informatico amministrativo
Durata conservazione:	Per 5 anni.
Liceità del trattamento	il trattamento è necessario per adempiere ad un obbligo legale al quale è soggetto il titolare del trattamento (art 6 comma 1 lettera C Reg. UE 679/16)

VALUTAZIONE DTMPATTO

Pencolo	Misure attuate	G	P	R
Distruzione	Protezione sistemi a cura del commercialista	b	B	B
Perdita	Protezione sistemi a cura del commercialista	B	B	B
Modifica	Protezione sistemi a cura del commercialista	B	B	B
Divulgazione non autorizzata	Protezione sistemi a cura del commercialista	B	B	B
Accesso accidentale o non autorizzato	Protezione sistemi a cura del commercialista	B	B	B

SCHEDA 3A	CATEGORIA INTERESSATI: DIPENDENTI E
Finalità del trattamento	RICERCA E SELEZIONE DEL PERSONALE

La ditta può richiedere o riceve curriculum da parte di soggetti interessati all'assunzione.

Dati trattati:	Identificativi e sensibili
Fonte.-	Forniti direttamente dall'interessato o da agenzie del lavoro
Destinatari:	Consulente del lavoro
Archivi:	Cartaceo o file informatici
Durata conservazione:	Per 6 mesi.
Liceità del trattamento	Il trattamento è necessario per adempiere ad un obbligo legale al miele è soggetto il titolare del trattamento art 6 comma 1 lettera C Reg. UE 679/16)

VALUTAZIONE DTMPATTO

Pericolo	Misure attuate	G	P	R
Distruzione	Copie conservate in archivi in cui sono eseguiti back up	B	B	B
Perdita	Copie conservate in archivi in cui sono eseguiti back up	B	B	B
Modifica	Generalmente i curriculum sono immodificabili	B	B	B
Divulgazione non autorizzata	Curriculum gestiti da addetto amministrazione	B	0	B
Accesso accidentale o non autorizzato	Curriculum gestiti da addetto amministrazione su aree provate	B	B	B

SCHEDA 3B	CATEGORIA INTERESSATI: DIPENDENTI E
Finalità del trattamento	GESTIONE AMMINISTRATIVA

Dati trattati per finalità amministrative (elaborazione contratti assunzione/dimissione e buste paga, gestione obblighi inerenti salute e sicurezza sul lavoro, gestione infortuni, accesso a sistemi informatici delle compagnie e iscrizioni/comunicazioni ad enti di controllo - IVASS o compagnie).

Dati trattati:	Identificativi, sensibili e giudiziari
Fonte:	Dati fomiti dall'interessato in fase di avviamento rapporto di lavoro
Destinatari:	Consulente del lavoro e Consulente Organizzazione Uffici pubblici del lavoro: IVASS;
Archivi:	Cartacei e archivi a cura del Responsabili esterni
Durata conservazione:	5 anni
Liceità del trattamento	Il trattamento è necessario per adempiere ad un obbligo legale al quale è soggetto il titolare del trattamento (art 6 comma 1 lettera C Reg. UE 679/16)

VALUTAZIONE D'IMPATTO

Pericolo	Misure attuate	G	P	R
Distruzione	Archivi cartacei protetti su armadi. Protezione archivi esterni a cura dei Responsabili esterni	B	B	B
Perdita	Archivi cartacei protetti su armadi. Protezione archivi esterni a cura dei	B	B	B
Modifica	Archivi cartacei protetti su armadi. Protezione archivi esterni a cura dei	B	B	B
Divulgazione non autorizzata	Archivi cartacei protetti su armadi. Protezione archivi esterni a cura dei Responsabili esterni	B	B	B
Accesso accidentale o non autorizzato	Archivi cartacei protetti su armadi. Protezione archivi esterni a cura dei Responsabili esterni	B	B	B

SCHEDA 3C	I - CATEGORIA INTERESSATI: DIPENDENTI E
Finalità del trattamento	I - SUPPORTO AL MARKETING

L'azienda, al fine di migliorare la comunicazione con la clientela, diffonde dati dei dipendenti per facilitarne il contatto, mediante:
Assegnazione di e-mail personale.
Inserimento della propria immagine su sito internet.

Dati trattati:	Identificativi, sensibili e giudiziari
Fonte:	Dati forniti dall'interessato in fase di avviamento rapporto di lavoro
Destinatari:	Consulente del lavoro e Consulente Organizzazione Uffici pubblici del lavoro: IVASS;
Archivi:	Cartacei e archivi a cura del Responsabili esterni
Durata conservazione:	5 anni
Liceità del trattamento	Il trattamento dei dati è lecito in seguito al consenso dell'interessato[art. b comma 1, lette a) Reg. UE 679/16)

VALUTAZIONE D'IMPATTO

Pericolo	Misure attuate	G	P	R
Distruzione	Dati protetti informaticamente e sui supporti cartacei	B	B	B
Perdita	Dati accessibili solo ad addetto amministrativo	B	B	B
Modifica	Modifiche accessibili solo da addetto amministrativo	B	B	B
Divulgazione non autorizzata	Divulgazione su siti internet autorizzato	B	B	B
Accesso accidentale o non autorizzato	Dati accessibili solo ad addetto amministrativo	0	B	B

SCHEDA 3D		CATEGORIA INTERESSATI: DIPENDENTI E COLLABORATORI		
Finalità del trattamento		VIDEOSORVEGLIANZA		
Ripresa e conservazione immagini di videosorveglianza per finalità di sicurezza locali.				
Dati trattati:	Immagini dei clienti			
Fonte:	Telecamere di videosorveglianza			
Destinatari:	Ufficiali di Pubblica Sicurezza			
Archivi:	hard disk dedicato			
Durata conservazione:	24 ore			
Liceità del trattamento	il trattamento dei dati è lecito m seguito al consenso dell'interessato (art. 6 comma 1, lette a) Reg. UE 679/16)			
VALUTAZIONE D'IMPATTO				
Pericolo	Misure attuate	G	P	R
Distruzione	Hard disk protetto da incendio	B	B	B
Perdita	Hard disk protetto	B	B	B
Modifica	Accesso hard disk solo con chiave	B	B	B
Divulgazione non autorizzata	Accesso hard disk solo a personale designato	B	B	B
Accesso accidentale o non autorizzato	Accesso hard disk solo a personale designato	B	B	B

Riepilogo dei rischi in materia di protezione dei dati degli interessati

Categoria di interessati		CLIENTI				
SCHEDA	Finalità trattamento	Rischio				
		Distruzione	Perdita	Modifica	Divulgazione non autorizzata	Accesso accidentale o illegale
1A	Attività amministrativa	BASSO	BASSO	BASSO	BASSO	BASSO
1B	Analisi adeguatezza assicurativa	BASSO	BASSO	BASSO	BASSO	BASSO
1C	Marketing Promozione di prodotti e servizi assicurativi	BASSO	BASSO	BASSO	BASSO	BASSO
1D	Videosorveglianza	BASSO	BASSO	BASSO	BASSO	BASSO

Categoria di interessati		FORNITORI				
SCHEDA	Finalità trattamento	Rischio				
		Distruzione	Perdita	Modifica	Divulgazione non autorizzata	Accesso accidentale o illegale
2A	Attività amministrativa	BASSO	BASSO	BASSO	BASSO	BASSO

Categoria di interessati		DIPENDENTI				
SCHEDA	Finalità trattamento	Rischio				
		Distruzione	Perdita	Modifica	Divulgazione non autorizzata	Accesso accidentale o illegale
3A	Ricerca e selezione del personale	BASSO	BASSO	BASSO	BASSO	BASSO
3B	Attività amministrativa	BASSO	BASSO	BASSO	BASSO	BASSO
3C	Supporto al marketing	BASSO	BASSO	BASSO	BASSO	BASSO
3D	Videosorveglianza	BASSO	BASSO	BASSO	BASSO	BASSO

Verifica rispetto requisiti minimi di sicurezza

11.1 Descrizione struttura archivi

Elenco attrezzature informatiche :

Tutti Personal computer, fax, scanner e stampanti come anche smartphone tablet e/o altri device, sono come da accordi, di proprietà della Compagnia Mandante che ne detiene elenco richiedibile presso la loro direzione centrale.
Gli hardware, i software fisici o online e le Configurazioni standard sono di proprietà e a cura delle compagnie Mandanti le quali ne hanno successivamente la cura e la vigilanza, la suddetta Agenzia è chiamata quindi, al ruolo di controllore al fine che gli utilizzi siano conformi alle specifiche mansioni e agli incarichi ricevuti da parte del Responsabile del trattamento dati ovvero il personale e i collaboratori della suddetta agenzia.

11.2 Protezione dati personali in formato elettronico

Sono adottati i seguenti accorgimenti minimi:

Inventario hardware e software

Gli hardware, i software fisici o online e le Configurazioni standard sono di proprietà e a cura della compagnie Mandanti le quali ne hanno successivamente la cura e la vigilanza, la suddetta Agenzia è chiamata quindi, al ruolo di controllore al fine che gli utilizzi siano conformi alle specifiche mansioni e agli incarichi ricevuti da parte del Responsabile del trattamento dati, in particolare, se sono presenti eventuali software di gestione dei dati dei clienti, questi saranno censiti tramite apposito Allegato al suddetto registro.

Gestione configurazione

La configurazione standard è definita dalle compagnie mandanti quali Titolari del Trattamento, ex art. 4 comma 7 GDPR, nessuna altra configurazione è consentita all'agenzia quale Responsabile del Trattamento, ex art. 4 comma 8 del GDPR.

Analisi della vulnerabilità

L'analisi della vulnerabilità secondo quanto previsto dagli artt. 32 e 35 del GDPR sono in capo al Titolare del Trattamento, per il suddetto caso sono le Compagnie di Assicurazione Mandanti ad assumere tale obbligo, la suddetta agenzia ha l'obbligo di essere conforme rispettare gli articoli presenti all'interno del Regolamento Europeo 679/2016 e le istruzioni eventualmente fornite da Responsabile.

Privilegi di Amministratore

L'amministratore di sistema o, tecnico sistemista di rete, è una figura professionale nominata e gestita dalla Compagnie Mandanti, in alcuni casi può essere anche sotto contratto in qualità di dipendente informatico presso le stesse. Tale figura si occupa di gestire gli Hardware e Software, oltre che le caratteristiche delle architetture informatiche e, in particolare, l'utilizzo e la condivisione di grandi quantità di dati attraverso le reti di comunicazione. Si occupa quindi essenzialmente di ogni tipo di rete informatica, comprese quelle a cui si accede via web, come le reti intranet, messe a disposizione della presente agenzia e implementa i sistemi di sicurezza del networking nonché definisce le procedure di autenticazione alla rete e di autorizzazione all'accesso ai dati da parte degli utenti, curando interventi di conservazione dei dati attraverso debite soluzioni di "backup" e progettando le attività di supporto al "disaster recovery" .

Antivirus e malware

Ogni dispositivo è protetto con antivirus, in dotazione da parte delle Compagnie mandanti già installati nelle apparecchiature in dotazione presso la suddetta agenzia, qualora si presenti casistica differente verrà annotata nel suddetto registro tramite appendice

Back up

Viene effettuato tramite l'amministratore di sistema o tramite processo automatizzato previsto dai software di proprietà delle Compagnie Mandanti, a loro è affidata la cura e la configurazione

Sistema di autenticazione informatica

I personal computer sono protetti da una password richiesta per ogni utente.
È presente uno screen-saver che obbliga il nuovo inserimento della password in caso di prolungato inutilizzo.
Tali credenziali sono modificate in automatico dall'Amministratore con frequenza semestrale.

Sistemi di autorizzazione

I sistemi di autorizzazione sono gestiti dai programmi e dagli operatori informatici dal Controllers quali le Compagnie Mandanti.

Sistemi per la protezione contro elementi esterni
I dispositivi sono protetti da firewall Microsoft, gestito direttamente dall'antivirus.
È inoltre presente un firewall di tipo fisico.

Protezione del server
Se presente, l'accesso al server è autorizzato al solo titolare e all'amministratore del sistema informatico.
L'accesso ai locali è impedito alle persone non autorizzate.
Il sistema è dotato inoltre di gruppo di continuità, che permette la protezione del sistema contro scariche atmosferiche, sbalzi di tensione e mancanza di energia temporanea.

Tutto il sistema è periodicamente sottoposto a manutenzione dall'Amministratore di Sistema delle Compagnie Mandanti.

11.3 Protezione dati personali in formato cartaceo

I documenti cartacei contenenti dati identificativi di clienti e dipendenti sono controllati e custoditi in armadio chiuso a chiave in modo da essere utilizzati solo dal personale autorizzato e per il tempo minimo necessario allo svolgimento delle operazioni di trattamento, al fine di evitare l'accesso alle persone prive di autorizzazione. I documenti sono contenuti all'interno di cartelle che impediscono di vederne il contenuto. L'identificazione di tali cartelle avviene mediante i soli dati identificativi attraverso un processo di anonimizzazione effettuato riportando il solo numero di polizza, gli addetti in ogni caso attuano delle procedure tali da evitare anche l'accesso involontario o indiretto ai dati da parte di terzi non autorizzati, riponendo immediatamente i documenti, in luogo sicuro e designato alla conservazione, in lavorazione e a loro affidati .

11.4 Protezione delle aree e dei locali

Contro i rischi di intrusione, sono adottati i seguenti accorgimenti:

- i locali sono dotati di porta con chiusura di sicurezza, gli armadi contenenti i dati sono chiudibili con lucchetti a chiave o simili;
- durante l'orario di apertura al pubblico sono poste restrizioni d'accesso delle persone non autorizzate (porta di accesso sempre chiusa con apertura dall'interno);
- le aree contenenti dati in supporto cartaceo sono lontane dalla zona dove sostano i clienti e sono comunque ubicate in modo tale che ciascun addetto possa rilevare a vista l'accesso da parte di estranei;
- i monitor, le stampanti i fax, i dispositivi quali smartphone e/o tablet in uso all'agenzia per attività e finalità di distribuzione assicurativa, affidati dalle Compagnie Mandanti, sono posizionati in modo da non consentire ad estranei la lettura o la sottrazione dei documenti;
- l'ufficio non si serve di addetti esterni alle pulizie, provvedendo in proprio; pertanto, non vi sono estranei che possano accedere ai locali al di fuori degli orari di apertura al pubblico. Qualora dovesse avvalersi di addetti esterni alle pulizie questi ultimi svolgono le operazioni in orari di lavoro o comunque sorvegliati da incaricati interni dell'agenzia, previa lettera di incarico adeguata alla loro mansione.
- l'ingresso dell'ufficio è attrezzato a sala d'aspetto isolata dagli uffici operativi cosicché chi è in attesa non ha accesso visivo ed acustico a quanto avviene negli altri locali. Comunque, in surrogazione nessuna trattativa, raccolta dati o informazione viene effettuata in presenza di Terzi non autorizzati, avvalendosi di luoghi, quali altre stanze dei locali, o postazioni lontane da essi.
-

11.5 Criteri e modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento

Le Compagnie Mandanti quali Responsabili hanno predisposto delle procedure a loro cura e verifica per il ripristino della disponibilità dei dati in seguito a distruzioni o danneggiamenti anche involontari.

13 Verifiche periodiche

Al fine di testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative presenti al fine di garantire la sicurezza del trattamento, l'agenzia si avvale della collaborazione di un professionista esterno:

AV CONSULTING ITALIA SRL
Sede legale: Via Privata del Gonfalone 3, 20123 Milano (MI)
e-mail: info@avconsultingitalia.it
pec : avconsulting@pec.avconsultingitalia.it

14 Violazione dei dati

Notifica all'autorità di controllo
In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente senza giustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Comunicazione all'interessato
Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza giustificato ritardo in conformità ed ottemperanza secondo quanto previsto dall'art.34 del GDPR. .

Tutte le violazioni dei dati sono opportunamente documentate in un "*Registro delle Violazioni dei dati*" c.d. "*Data Breach*" – contenuto all'interno del fascicolo "*Sistema Gestione Compliance*" nella sezione "*Privacy".*

15 Documenti a supporto:

- Documento 1: Autorizzazione al trattamento dati mediante lettera di incarico contenuta all'interno del fascicolo "Sistema Gestione Compliance" nella sezione "Fascicoli Personale"
- Documento 2: Elenco Istruzioni / procedure delle Compagnie disponibili, consultabili e scaricabili presso intranet agenziale o tramite piattaforma della Compagni.
- Documento 3: Registro delle Violazioni dei dati c.d. "Data Breach" contenuto all'interno del fascicolo "Sistema Gestione Compliance" nella sezione "Privacy".