REGISTRO
DELLE ATTIVITA' DI TRATTAMENTO

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

IN QUALITA' DI
TITOLARE DEL TRATTAMENTO

Agenzia di assicurazioni
ANNICCHIARICO ASSICURAZIONI S.R.L.
GALLERIA CRISTALLO 16/3
RAPALLO (GE)

Data di emissione: 10.02.2025

Documento composto da 34 pagine
Revisione 8

Il Titolare del Trattamento

Firmato da: ANNICCHIARICO ANDREA NNCNDR64S11D969C AG15568*80
EMail: andrea.annicchiarico.39190@unipolsai.it
Ora/data firma: 12-02-2025 13:52:23
Indirizzo IP: 88.37.152.112

AG15568*40

1 Introduzione

La società ANNICCHIARICO ASSICURAZIONI S.R.L. ha mandati agenziali di intermediazione assicurativa da parte di compagnie di assicurazione.
L'attività di intermediazione consiste nel proporre e stipulare prodotti assicurativi delle compagnie mandanti, rispettando i regolamenti IVASS in materia di intermediazione assicurativa, che impongono obbligatoriamente specifici trattamenti, anche al fine di valutare l'adeguatezza di un contratto o valutare il rischio di riciclaggio di denaro.
Normative obbligatorie sono:

- D.Lgs. 209/05 Codice delle assicurazioni private, e relativi regolamenti IVASS
- D.Lgs 231/07 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

A tal fine, l'agenzia opera in qualità di Responsabile del Trattamento dati, i cui Titolari del Trattamento dati sono le compagnie mandanti. In tale ruolo, quindi, la ditta ha elaborato un "*Registro delle attività di trattamento in qualità di Responsabile*" secondo quanto indicato dalle 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 presente documento si riferisce al solo trattamento dati svolto in qualità di autonomo Titolare.

2 Definizioni

Regolamento: 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, che abroga la direttiva 95/46/CE (GDPR - Regolamento Generale sulla Protezione dei Dati);

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;

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;

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;

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;

Responsabile della Protezione dei Dati ("DPO" o "RPD"): soggetto autonomo e indipendente nei confronti dell'azienda insignito di funzioni di supporto, controllo, consultazione, formazione e informazione per quanto attiene alla corretta applicazione del GDPR.

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.

Autorizzato: le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare del trattamento o dal Responsabile del trattamento;

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 del trattamento o del responsabile del trattamento

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;

3 Ambito di applicazione e norme di riferimento

In qualità di Titolare del trattamento, l'agenzia ritiene fondamentale, nello svolgimento delle proprie attività, il rispetto dei seguenti principi:

- Il trattamento dei dati degli interessati, in particolare dei propri dipendenti, collaboratori e dei propri clienti deve avvenire nel pieno rispetto dei loro diritti.
- Il trattamento dei dati personali deve essere eseguito in pieno accordo al Regolamento Europeo sulla Privacy UE 2016/679.

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 degli interessati.
- È vietato il trasferimento di dati personali verso paesi terzi.
- Le misure di sicurezza definite per la protezione dei dati devono essere attuate da tutto il personale agenziale.

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.

La presente Agenzia non dispone di videosorveglianza

Sito web: www.annicchiaricoassicurazioni.it

Norme di riferimento

Tutela dati personali:

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);

DECRETO LEGISLATIVO 30 giugno 2003, n.196 recante il "Codice in materia di protezione dei dati personali";

DECRETO LEGISLATIVO 10 agosto 2018, n.101;

PROVVEDIMENTI EMANATI DAL GARANTE per la protezione dei dati personali

- Semplificazioni di taluni adempimenti in ambito pubblico e privato rispetto a trattamenti per finalità amministrative e contabili - 19 giugno 2008;

- Provvedimento 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 Generale del Garante per la protezione dei dati personali dell'8 aprile 2010 in tema di "Videosorveglianza" e "FAQ in tema di videosorveglianza e protezione dei dati personali", pubblicate a dicembre 2020;

- Provvedimento del Garante sulla notifica delle violazioni dei dati personali (data breach) - 30 luglio 2019;

LINEE GUIDA DEL GARANTE

- Linee guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del Regolamento 2016/679 (Working Party 248)

- Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video

- Linee guida cookie e altri strumenti di tracciamento del 10 giugno 2021

Cyber security:

REGOLAMENTO UE 2019/881 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del 17 aprile 2019 relativo all'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cybersicurezza»)

NORMATIVA SECONDARIA EMANATA DA IVASS

- Lettera al mercato del 29 dicembre 2017 – Esiti dell'indagine conoscitiva sui presidi degli intermediari tradizionali per la gestione delle informazioni e la prevenzione dei rischi informatici.

Indicazioni per gli intermediari

Sicurezza informatica:

Semplificazione delle misure di sicurezza contenute nel disciplinare tecnico di cui all'Allegato B) al Codice in materia di protezione dei dati personali - 27 novembre 2008

4 Ruoli

Titolare del Trattamento:

- Nome e Cognome /denomin. sociale: ANNICCHIARICO ASSICURAZIONI S.R.L.
- Indirizzo: GALLERIA CRISTALLO 16/3 - RAPALLO (GE)
- Telefono, Fax: 0185234101
- Email / PEC: annicchiaricoassicurazionisrl@gmail.com - annicchiaricoassicurazionisrl@legalmail.it

L'agenzia si avvale, per il trattamento dei dati per finalità operative, di:
- DIPENDENTI:
  Personale assunto con contratto di lavoro subordinato basato su contratti nazionali.
- STAGISTI / TIROCINANTI:
  Vincolati da contratto di stage / tirocinio.
- COLLABORATORI:
  Personale esterno senza vincolo di subordinazione vincolati da un mandato.

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 l'**Allegato 1,** firmato in apposito fascicolo.

Il personale ivi indicato è istruito direttamente dal titolare del trattamento dati mediante corsi di formazione dedicati, valevoli e obbligatori anche ai fini IVASS.

L'istruzione operativa 02 definisce la modalità di fornire adeguata informazione a tali collaboratori.

La struttura organizzativa indica l'elenco degli autorizzati.

L'agenzia, per il trattamento dati per finalità amministrative, si avvale inoltre della collaborazione di:
- Professionisti:
  Consulenti del lavoro, Commercialisti e consulenti in organizzazione.
- Fornitori di servizi
  Fornitori di manutenzione dei sistemi informatici, fornitori di software aziendali, eventuali società per campagne marketing o per la gestione delle mail o del sito internet.

Tali figure sono nominate Responsabili del Trattamento dati, mediante **Allegato 2** o documento equivalente concordato tra le parti, che fornisce anche istruzioni di base in materia di obblighi previsti. Per alcune figure che svolgono ordinaria attività di gestione amministrativa e contabile non si è ritenuto necessario nominarli Responsabili del Trattamento dati in quanto si ritengono

adempimenti superflui o ripetuti inutilmente da cui non deriva un reale valore aggiunto ai fini della correttezza e della trasparenza del trattamento come previsto dal Garante con provvedimento pubblicato in *Gazzetta Ufficiale 1° luglio 2008, n. 152.*

Elenco Responsabili del trattamento:

Consulenza gestionale	K PARTNERS SRL
Consulente del lavoro	STUDIO CAUZZI - Via della libertà 67 - 1
Commercialista	DOTT.SSA TRAVERSO DANIELA - Via R.C. Ceccardi 3/5 16121 Genova (GE)
Sistema informatico	SAVE S.RL.
Assistenza hardware	G3 SYSTEM DI EROS GIANNOTTA
Digitalizzazione esterna documenti	GSV
Gestore account per le mail aziendali	
Gestore creazione utenze portali di lavoro	

Per la gestione della sicurezza sul lavoro i dati sono trattati anche dalla società che cura gli adempimenti sulla normativa in vigore.

Responsabile della Protezione dei Dati

Per le finalità indicate nel presente documento, l’agenzia non ha assegnato l'incarico di Responsabile della protezione dei dati, in quanto non sono soddisfatti i requisiti necessari previsti all’articolo 37 comma 1 del Regolamento Europeo 2016-679 che ne prevedono l’obbligo. Al fine di presidiare i processi in materia privacy può essere nominato un Referente privacy. Qualora non presente tale incarico sarà affidato a ANNICCHIARICO ASSICURAZIONI S.R.L. in qualità di Titolare del Trattamento dati. Nel caso in cui sia nominato è presente il documento che ne stabilisce le responsabilità.

Amministratore di sistema

Si individuano generalmente, in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Vengono considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi”.

Incaricati al Trattamento dati

Le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare del trattamento o del responsabile del trattamento.

Sub-Responsabili

Il sub-responsabile del trattamento è una figura che può essere nominata dal responsabile del trattamento per assisterlo o sostituirlo nel trattamento dei dati personali.

Quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento.

4 Categorie di interessati, finalità e liceità

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, appartenenti a categorie particolari, per adempiere agli obblighi di legge in materia di contabilità e fiscalità, per finalità connesse all’attività di consulenza, distribuzione assicurativa e di altre attività accessorie.

Liceità: il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso

Finalità 1B: *Analisi esigenze assicurative*

L’agenzia di assicurazione acquisisce una serie di informazioni dei clienti o dei potenziali clienti al fine di valutare i prodotti assicurativi più coerenti alle loro esigenze, secondo quanto previsto dai regolamenti obbligatori applicabili all’attività di intermediazione assicurativa, anche acquisendo e conservando copia delle polizze assicurative

Liceità: il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso.

Finalità 1C: *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.

Liceità: il trattamento è necessario per il perseguimento del legittimo interesse

Categoria di interessati: FORNITORI

I fornitori dell’agenzia di assicurazione forniscono prodotti e servizi necessari per il funzionamento amministrativo.

Finalità 2A: *Attività amministrative*
Sono trattati i dati dei fornitori per svolgere gli adempimenti amministrativi in termini fiscali.

Liceità: il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte

Categorie di interessati: DIPENDENTI E COLLABORATORI

Costituiscono gli addetti, dipendenti e collaboratori, all'attività di intermediazione e alle attività amministrative.

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

Liceità: l'interessato ha espresso il consenso al trattamento dei propri dati personali

Finalità 3B: *Attività amministrative*
- Svolgimento di adempimenti civilistici, contabili, fiscali e regolamentari.
- Creazione di utenze per i portali sia dell'agenzia che delle Compagnie con cui hanno accordi diretti o eventuali mail aziendali per l'attività lavorativa.
- Svolgimento attività previste da obblighi di legge in materia di intermediazione assicurativa e per finalità connesse all'attività di consulenza distribuzione assicurativa e di altre attività accessorie.

Liceità: il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento

Finalità 3C: *Supporto al Marketing*
Diffusione alla clientela, su sistemi di comunicazione locale e nazionale (es. sito internet, riviste di settore, tv e social network), di dati personali degli addetti (immagini e video) per facilitarne la comunicazione. Inoltre, potranno essere utilizzati per promuovere e organizzare eventi dell'agenzia.

Liceità: l'interessato ha espresso il consenso al trattamento dei propri dati personali

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

Liceità: il trattamento è necessario per il perseguimento del legittimo interesse

6 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 esigenze assicurative	Identificativi Prodotti assicurativi acquistati Dati idonei a valutare la coerenza dei contratti offerti	X	X	-
	1C - Videosorveglianza	Identificativi, quali immagini o video	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		

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

7 Categorie di destinatari

Categorie di interessati	Finalità trattamento	Categorie di destinatari
CLIENTI	1A - Attività amministrativa	Commercialista Software aziendali
	1B - Analisi coerenza assicurativa	Compagnie di assicurazione Altri intermediari assicurativi
	1C- Videosorveglianza	Ufficiali di Pubblica Sicurezza
FORNITORI	2A - Attività amministrativa	Commercialista
DIPENDENTI E COLLABORATORI	3A – Ricerca e selezione del personale	Società di ricerca e selezione del personale
	3B - Attività amministrative	Consulente del lavoro Consulente Organizzazione Software aziendali interni
	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.

8 Termini ultimi di cancellazione

Categorie di interessati	Finalità trattamento	Termine ultimo di cancellazione
CLIENTI	1A - Attività amministrativa	10 anni secondo leggi fiscali
	1B - Analisi esigenze assicurative	10 anni per difesa in giudizio su attività professionale 5 anni di conservazione obbligatoria in materia Ivass
	1C- Videosorveglianza	24 ore
FORNITORI	2A - 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 Utenze o mail aziendali vengono disattivate alla cessazione del rapporto
	3C - Supporto all’attività di marketing agenziale	Alla cessazione del rapporto di lavoro
	3D - Videosorveglianza locali	24 ore

9 Misure di sicurezza tecniche ed organizzative

Di seguito è riportato l'elenco delle istruzioni riportanti le misure tecniche ed organizzative messe in atto per garantire un corretto trattamento dei dati degli interessati:

Istruzioni operative:

Istruzione 01 - Attività amministrativa

Istruzione 02 - Intermediazione assicurativa

Istruzione 03 - Svolgimento attività di marketing

Istruzione 04 - Comunicazione a soggetti terzi

Istruzione 05 - Videosorveglianza in agenzia

Istruzione 06 - Gestione del personale

Altre misure tecniche ed organizzative attuate:

Istruzione 07 – gestione delle modifiche ai mezzi di trattamento

Istruzione 08 – gestione delle richieste degli interessati

Istruzione 09 – segnalazione violazioni di privacy

Altre misure in materia di sicurezza informatica

Istruzione 10 - Regolamento per l'utilizzo della rete

Istruzione 11 - Regole di comportamento per minimizzare i rischi da virus

Istruzione 12 - Regole per la Gestione delle password

Istruzione 13 - Regole sicurezza informatica

10 Istruzioni operative

Istruzione 01 - Attività amministrativa

I documenti cartacei devono essere conservati in armadio chiuso a chiave in area amministrazione o rieservata, a cui può accedere solo l'incaricato amministrativo.

Istruzione 02 - Intermediazione assicurativa

L’attività primaria di intermediazione assicurativa deve essere condotta secondo le istruzioni impartite dalla Compagnia, che assume il ruolo di Titolare del trattamento dati.

Tutti i dipendenti e collaboratori che svolgono l’attività di intermediazione assicurativa, devono procedere a informare i clienti del trattamento dati in qualità di responsabili e far firmare il consenso al trattamento per la finalità di intermediazione assicurativa e marketing nell’informativa privacy.
Deve essere inoltre fleggato su tale sistema informatico di Compagnia l’avvenuta acquisizione del consenso.

Comunicazioni tramite email:

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.

Istruzione 03 – Svolgimento attività di Marketing

Le attività di promozione commerciale di prodotti assicurativi deve avvenire nel pieno rispetto delle istruzioni indicate nei relativi corsi di formazione e dopo aver raccolto il consenso da parte dei clienti.
In particolare:

- E’ fatto divieto di contattare un interessato senza preventivo consenso per l’attività di marketing.
- E’ fatto divieto di usare dati sensibili per attività di marketing e profilazione.
- E' fatto divieto svolgere profilazione dei clienti.

Marketing tramite siti internet:

Se presente devono essere rispettate le normative in materia di cookies nella pagina iniziale (allegato 21 fornisce un esempio di testo).
Se presenti form di richiesta informazioni, deve essere fornita adeguata informativa privacy (allegati 22a e 22b per i testi da inserire).
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 email, deve essere loro fornita adeguata informativa secondo l'**allegato 25.**

Istruzione 04 – Comunicazioni a soggetti terzi

I dati dei clienti potranno essere trattati per finalità di comunicazione a Società del Gruppo (società controllanti, controllate e collegate, anche indirettamente, ai sensi delle vigenti disposizioni di legge), a soggetti operanti nel settore delle telecomunicazioni, nei servizi bancari, finanziari, assicurativi e IT (Information Technology), nell'ambito della vendita diretta di beni e servizi, che li tratteranno per proprie finalità di pubblicità e di marketing sia attraverso strumenti tradizionali (per esempio, posta cartacea e/o chiamate con operatore, etc.), sia per il tramite di strumenti di comunicazione elettronica quali e-mail, fax, SMS, MMS.

Istruzione 05 – Inserimento Videosorveglianza in agenzia

Se presente per attivare l'impianto videosorveglianza è necessario:

- Predisporre le informative ai dipendenti sull'intenzione di installare un impianto di videosorveglianza (**allegato 31**)
- Incaricare un Designato all'accesso dei dati di videosorveglianza (**allegato 32**)
- Predisporre la domanda all'ispettorato del lavoro (**allegato 33**)
- Predisporre la comunicazione ai dipendenti dell'attivazione dell'impianto di videosorveglianza (**allegato 34**)
- Tutte le aree sottoposte a videosorveglianza devono poi essere adeguatamente segnalate (**allegato 35**)
- Qualora subentrassero nuovi dipendenti è necessario far sottoscrivere l'informativa, area videosorvegliata (**allegato 36**)

Senza autorizzazione dell'ispettorato del lavoro le telecamere di videosorveglianza NON possono essere attivate.

Nel caso in cui vi sia una richiesta da parte dell'autorità di controllo competente delle registrazioni, l'incaricato all'accesso si riserva la facoltà di conservare una copia.

Istruzione 06 - Gestione del personale

Ricerca personale

L'addetto/a amministrazione riceve i curriculum dei candidati in formato cartaceo o elettronico.
E' 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 form di contatto per invio curriculum, deve essere fornita adeguata informativa come da **allegato 24**.

Assunzione personale

In fase assuntiva, l'addetto/a amministrazione fornisce l'informativa privacy (**allegato 3**) al dipendente/collaboratore e, se necessario, richiede il consenso per il trattamento dati per finalità specifiche:

- Videosorveglianza (vedi istruzione 05)
- Marketing su siti internet (vedi istruzione 03)

Qualora presente viene inoltre consegnato il Regolamento Aziendale (**allegato 5**), una cui copia deve essere firmata per presa visione ed accettazione.
I dati vengono comunicati anche alla società che gestisce gli adempimenti sulla sicurezza del lavoro .
Qualora il dipendente/collaboratore non avesse svolto adeguati corsi di formazione in materia di privacy, l'addetto/a amministrazione procede a richiedergli tale 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.

Censimento interno

In fase inziale di censimento, vengono usati i dati degli addetti per la creazione di utenze univoche per i portali interni creati da , potrebbero essere usati i dati per creare apposite mail aziendali personalizzate.

Conclusione rapporto di collaborazione

In fase di cessazione del rapporto di collaborazione:
- Cancellare tutti i dati di marketing (dal sito internet, in brochure,…)
- Le utenze sono disattivate alla chiusura del rapporto
- Eventuali mail aziendali personalizzate vengono disabilitate e eliminare in tempi congrui a gestire il passaggio ad altri membri della rete aziendale
- Prendere cartellina personale e posizionarla nell'archivio morto, prevedendone la distruzione

Istruzione 07 – 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 08 – Gestione richieste degli interessati

Gli interessati possono precedere alle seguenti richieste:

RICHIESTA	AZIONE
Comunicare ai propri destinatari rettifiche o cancellazioni richieste	Mandare email 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 email, 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 accettato, 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, 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 09 – 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, nella persona degli Agenti all'indirizzo email agenziale e comunque non oltre le 72 ore.

Questi, provvederà immediatamente a segnalare la violazione come indicato al successivo punto 13.

Istruzione 10 – Regolamento per l'utilizzo della rete

Oggetto e ambito applicazione

Il presente regolamento disciplina le modalità di accesso e di uso della rete informatica e

telematica e dei servizi che, tramite la stessa rete, è possibile ricevere o offrire.

Principi Generali – diritti e responsabilità

L'agenzia promuove l'utilizzo della rete quale strumento utile per perseguire le proprie finalità.
Gli utenti manifestano liberamente il proprio pensiero nel rispetto dei diritti degli altri utenti e di terzi, nel rispetto dell'integrità dei sistemi e delle relative risorse fisiche, in osservanza delle leggi, norme e obblighi contrattuali.
Consapevoli delle potenzialità offerte dagli strumenti informatici e telematici, gli utenti si impegnano ad agire con responsabilità e a non commettere abusi aderendo a un principio di autodisciplina.
Il posto di lavoro costituito da personal computer viene consegnato completo di quanto necessario per svolgere le proprie funzioni, pertanto è vietato modificarne la configurazione.
Il software installato sui personal computer è quello richiesto dalle specifiche attività lavorative dell'operatore. E' pertanto proibito installare qualsiasi programma da parte dell'utente o di altri operatori, escluso l'amministratore del sistema. L'utente ha l'obbligo di accertarsi che gli applicativi utilizzati siano muniti di regolare licenza.
Ogni utente è responsabile dei dati memorizzati nel proprio personal computer. Per questo motivo è tenuto ad effettuare la copia di questi dati secondo le indicazioni emanate dal titolare del trattamento dei dati o suo delegato.

Abusi e Attività Vietate

E' vietato ogni tipo di abuso. In particolare, è vietato:

- usare la rete in modo difforme da quanto previsto dalle leggi penali, civili e amministrative e da quanto previsto dal presente regolamento;
- utilizzare la rete per scopi incompatibili con l'attività istituzionale;
- utilizzare una password a cui non si è autorizzati;
- cedere a terzi codici personali (USER ID e PASSWORD) di accesso al sistema;
- conseguire l'accesso non autorizzato a risorse di rete interne o esterne;
- violare la riservatezza di altri utenti o di terzi;
- agire deliberatamente con attività che influenzino negativamente la regolare operatività della rete e ne restringano l'utilizzabilità e le prestazioni per altri utenti;
- agire deliberatamente con attività che distraggano risorse (persone, capacità, elaboratori);
- fare o permettere ad altri, trasferimenti non autorizzati di informazioni (software, basi dati, ecc.);
- installare o eseguire deliberatamente o diffondere su qualunque computer e sulla rete, programmi destinati a danneggiare o sovraccaricare i sistemi o la rete (p.e. virus, cavalli di troia, worms, spamming della posta elettronica, programmi di file sharing - p2p);
- installare o eseguire deliberatamente programmi software non autorizzati e non compatibili con le attività istituzionali;
- cancellare, disinstallare, copiare, o asportare deliberatamente programmi software per scopi personali;
- installare deliberatamente componenti hardware non compatibili con le attività istituzionali;
- rimuovere, danneggiare deliberatamente o asportare componenti hardware.
- utilizzare le risorse hardware e software e i servizi disponibili per scopi personali;
- utilizzare le caselle di posta elettronica per scopi personali e/o non istituzionali;
- utilizzare la posta elettronica con le credenziali di accesso di altri utenti;
- utilizzare la posta elettronica inviando e ricevendo materiale che violi le leggi.

- utilizzare l'accesso ad Internet per scopi personali;
- accedere direttamente ad Internet con modem collegato al proprio Personal Computer se non espressamente autorizzati e per particolari motivi tecnici;
- connettersi ad altre reti senza autorizzazione;
- monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività degli utenti, leggere copiare o cancellare file e software di altri utenti, senza averne l'autorizzazione esplicita;
- usare l'anonimato o servirsi di risorse che consentano di restare anonimi sulla rete;
- inserire o cambiare la password del bios, se non dopo averla espressamente comunicata all'amministratore di sistema e essere stati espressamente autorizzati;
- abbandonare il posto di lavoro lasciandolo incustodito o accessibile, come specificato nell'allegato 3.

Attività consentite

E' consentito all'amministratore di sistema:

- monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare il corretto utilizzo delle risorse di rete, dei clienti e degli applicativi, per copiare o rimuovere file e software, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;
- creare, modificare, rimuovere o utilizzare qualunque password, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori. L'amministratore darà comunicazione dell'avvenuta modifica all'utente che provvederà ad informare il custode delle password come da procedura descritta nell'allegato 3;
- rimuovere programmi software, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;
- rimuovere componenti hardware, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori.

Soggetti che possono aver accesso alla rete

Hanno diritto ad accedere alla rete tutti i dipendenti, le ditte fornitrici di software per motivi di manutenzione e limitatamente alle applicazioni di loro competenza, collaboratori esterni impegnati nelle attività istituzionali per il periodo di collaborazione.
L'accesso alla rete è assicurato compatibilmente con le potenzialità delle attrezzature.
L'amministratore di sistema può regolamentare l'accesso alla rete di determinate categorie di utenti, quando questo è richiesto da ragioni tecniche.
Per consentire l'obiettivo di assicurare la sicurezza e il miglior funzionamento delle risorse disponibili, l'amministratore di sistema può proporre al titolare del trattamento l'adozione di appositi regolamenti di carattere operativo che gli utenti si impegnano ad osservare.
L'accesso agli applicativi è consentito agli utenti che, per motivi di servizio, ne devono fare uso.

Modalità di accesso alla rete e agli applicativi

Qualsiasi accesso alla rete e agli applicativi viene associato ad una persona fisica cui collegare le attività svolte utilizzando il codice utente.
L'utente che ottiene l'accesso alla rete e agli applicativi si impegna ad osservare il presente

regolamento e le altre norme disciplinanti le attività e i servizi che si svolgono via rete e si impegna a non commettere abusi e a non violare i diritti degli altri utenti e dei terzi.
L'utente che ottiene l'accesso alla rete e agli applicativi si assume la totale responsabilità delle attività svolte tramite la rete.
L'utente è tenuto a verificare l'aggiornamento periodico del software antivirus.
Al primo collegamento alla rete e agli applicativi, l'utente deve modificare la password (parola chiave)
comunicatagli dal custode delle password e rispettare le norme indicate nell'allegato 3.

Sanzioni

In caso di abuso, a seconda della gravità del medesimo, e fatte salve ulteriori conseguenze di natura penale, civile e amministrativa, possono essere comminate le sanzioni disciplinari previste dalla normativa vigente in materia e dai regolamenti interni.

Istruzione 11 – Regole di comportamento per minimizzare i rischi da virus

---

Per minimizzare il rischio da virus informatici, gli utilizzatori dei PC adottano le seguenti regole:
• divieto di lavorare con diritti di amministratore o superutente sui sistemi operativi che supportano la multiutenza;
• limitare lo scambio fra computer di supporti rimovibili (floppy, cd, zip) contenenti file con estensione EXE, COM, OVR, OVL, SYS, DOC , XLS;
• controllare (scansionare con un antivirus aggiornato) qualsiasi supporto di provenienza sospetta prima di operare su uno qualsiasi dei file in esso contenuti;
• evitare l'uso di programmi shareware e di pubblico dominio se non se ne conosce la provenienza, ovvero divieto di “scaricare“ dalla rete internet ogni sorta di file, eseguibile e non. La decisione di “scaricare” può essere presa solo dall'amministratore di sistema;
• disattivare la creazione di nuove finestre ed il loro ridimensionamento e impostare il livello di protezione su “chiedi conferma” (il browser avvisa quando uno script cerca di eseguire qualche azione);
• attivare la protezione massima per gli utenti del programma di posta Outlook Express (o altro gestore) al fine di proteggersi dal codice html di certi messaggi e-mail (buona norma è visualizzare e trasmettere messaggi in formato testo poiché alcune pagine web, per il solo fatto di essere visualizzate possono infettare il computer);
• non aprire gli allegati di posta se non si è certi della loro provenienza, e in ogni caso analizzarli con un software antivirus. Usare prudenza anche se un messaggio proviene da un indirizzo conosciuto (alcuni virus prendono gli indirizzi dalle mailing list e della rubrica di un computer infettato per inviare nuovi messaggi "infetti");
• non cliccare mai un link presente in un messaggio di posta elettronica da provenienza sconosciuta,(in quanto potrebbe essere falso e portare a un sito-truffa);
• non utilizzare le chat;
• consultare con periodicità settimanale la sezione sicurezza del fornitore del sistema operativo e applicare le patch di sicurezza consigliate;
• non attivare le condivisioni dell'HD in scrittura.
• seguire scrupolosamente le istruzioni fornite dal sistema antivirus nel caso in cui tale sistema antivirus abbia scoperto tempestivamente il virus (in alcuni casi esso è in grado di risolvere il problema, in altri chiederà di eliminare o cancellare il file infetto);
• avvisare l'Amministratore di sistema nel caso in cui il virus sia stato scoperto solo dopo aver subito svariati malfunzionamenti della rete o di qualche PC, ovvero in ritardo (in questo caso è

possibile che l'infezione abbia raggiunto parti vitali del sistema);
• conservare i dischi di ripristino del proprio PC (creati con l'installazione del sistema operativo, o forniti direttamente dal costruttore del PC);
• conservare le copie originali di tutti i programmi applicativi utilizzati e la copia di backup consentita per legge;
• conservare la copia originale del sistema operativo e la copia di backup consentita per legge;
• conservare i driver delle periferiche (stampanti, schede di rete, monitor ecc. fornite dal costruttore).

Nel caso di sistemi danneggiati seriamente da virus l'Amministratore e/o il tecnico esterno incarico dell'assistenza procede a reinstallare il sistema operativo, i programmi applicativi ed i dati; seguendo la procedura indicata:

• formattare l'Hard Disk, definire le partizioni e reinstallate il Sistema Operativo. (molti produttori di personal computer forniscono uno o più cd di ripristino che facilitano l'operazione);
• installare il software antivirus, verificare e installare immediatamente gli eventuali ultimi aggiornamenti;
• reinstallare i programmi applicativi a partire dai supporti originali;
• effettuare il RESTORE dei soli dati a partire da una copia di backup recente. NESSUN PROGRAMMA ESEGUIBILE DEVE ESSERE RIPRISTINATO DALLA COPIA DI BACKUP: potrebbe essere infetto;
• effettuare una scansione per rilevare la presenza di virus nelle copie dei dati;
• ricordare all'utente di prestate particolare attenzione al manifestarsi di nuovi malfunzionamenti nel riprendere il lavoro di routine.

Istruzione 12 – Regole per la Gestione delle password

Tutti gli incaricati del trattamento dei dati personali accedono al sistema informativo per mezzo di un codice identificativo personale (in seguito indicato User-id) e password personale.
User-id e password iniziali sono assegnati a .
User-id e password sono strettamente personali e non possono essere riassegnati ad altri utenti.
La password è composta da 8 caratteri alfanumerici. Detta password non contiene, né conterrà, elementi facilmente ricollegabili all'organizzazione o alla persona del suo utilizzatore.
Ogni tre mesi il sistema richiede automaticamente il cambio delle password di accesso; ciascun incaricato provvede a sostituire la propria password e a comunicare la variazione effettuata da .
Le password di amministratore di tutti i PC che lo prevedono sono assegnate dall'amministratore di sistema, esse sono conservate in busta chiusa nella cassaforte. In caso di necessità l'amministratore di sistema è autorizzato a intervenire sui personal computer.
In caso di manutenzione straordinaria possono essere comunicate, qualora necessario, dall'amministratore di sistema al tecnico/sistemista addetto alla manutenzione le credenziali di autenticazione di servizio. Al termine delle operazioni di manutenzione l'amministratore di sistema deve ripristinare nuove credenziali di autenticazione che devono essere custodite in cassaforte.
Le disposizioni di seguito elencate sono vincolanti per tutti i posti lavoro tramite i quali si può accedere alla rete e alle banche dati contenenti dati personali e/o sensibili:
le password assegnate inizialmente e quelle di default dei sistemi operativi, prodotti software, ecc. devono essere immediatamente cambiate dopo l'installazione e al primo utilizzo;
per la definizione/gestione della password devono essere rispettate le seguenti regole:

• la password deve essere costituita da una sequenza di minimo otto caratteri alfanumerici e non

deve essere facilmente individuabile;
• deve contenere almeno un carattere alfabetico ed uno numerico;
• non deve contenere più di due caratteri identici consecutivi;
• non deve contenere la user-id come parte della password;
• al primo accesso la password ottenuta dal custode delle password deve essere cambiata;
• la nuova password non deve essere simile alla password precedente;
• la password deve essere cambiata almeno ogni sei mesi, tre nel caso le credenziali consentano l'accesso ai dati sensibili o giudiziari;
• la password termina dopo sei mesi di inattività;
• la password è segreta e non deve essere comunicata ad altri;
• la password va custodita con diligenza e riservatezza;
• l'utente deve sostituire la password, nel caso ne accertasse la perdita o ne verificasse una rivelazione surrettizia.

Istruzione 13 – Regole di sicurezza informatica

Ruoli e responsabilità
Per le finalità indicate nel presente documento, la ditta conferisce la responsabilità IT e information Security all'agente in qualità di responsabile dell'attività di intermediazione assicurativa. Tale figura può essere affiancata da un amministratore di sistema interno o esterno con apposito incarico. In tal caso, si rimanda al contratto stipulato con l'amministratore di sistema l'elencazione analitica degli ambiti di operatività consentiti e le responsabilità.
L'agente si impegna annualmente alla compilazione dell'allegato 1 della policy cyber security aziendale. Si rinvia la responsabilità all'amministratore di sistema interno o esterno nel caso in cui venga incaricato per la compilazione dell'allegato.

Inventario hardware e software
è necessario che l'incaricato si dedichi alla gestione e alla manutenzione di impianti di elaborazioni con cui vengono effettuati trattamento dati personali, compresi i sistemi di gestione delle base dei dati, i sistemi software complessi, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali. Viene redatto l'inventario dei dispositivi hardware e software, che dev'essere aggiornato periodicamente. Devono essere indicati i dispositivi fisici (hardware) e i programmi (software), con le rispettive licenze, e tutti i sistemi, i servizi e le applicazioni informatiche utilizzate all'interno dell'azienda. Per quanto riguarda le applicazioni, i sistemi informatici e i programmi in uso forniti da terze parti (spazi web, servizi cloud, social network e posta elettronica) devono essere ridotti a quelli strettamente necessari per lo svolgimento dell'attività dell'impresa. È necessario aggiornare l'inventario quando ci sono nuovi dispositivi e software installati o collegati alla rete. Per i dispositivi che possiedono un indirizzo IP l'inventario deve indicare i nomi delle macchine e la funzione del sistema. L'inventario deve includere dispostivi come telefoni cellulari, tablet e laptot e altri dispositivi elettronici portatili che memorizzano o elaborano dati. Tali mansioni se non conferite ad un amministratore di sistema interno o esterno spettano all'Agente.

Gestione della configurazione dei PC
La configurazione è necessaria affinché i programmi installati nel PC possano funzionare correttamente. L'incaricato compila la scheda controllo sicurezza informatica. Devono essere individuati il numero dei PC, il sistema operativo, l'indicazione dell'aggiornamento periodico e l'amministratore di sistema. Inoltre, dev'essere presente lo screen saver, il back up periodico e l'antivirus.

Analisi della vulnerabilità
La vulnerabilità informatica del software è la segnalazione di una falla in un computer. è necessario analizzare se i dispositivi sono protetti da virus, malware e tentativi di intrusione. I PC devono essere dotati di Antivirus. È vietato installare o eseguire deliberatamente o diffondere su qualunque computer e sulla rete, programmi destinati a danneggiare o sovraccaricare i sistemi o la rete e utilizzare la rete per scopi connessi all'attività designata. Abusi e attività vietate sono sopra descritte nelle istruzioni.

Verifica installazione e aggiornamenti antivirus
L'incaricato verifica che tutti i dispositivi mobili siano dotati di Antivirus. L'antivirus installato viene indicato nell'allegato 1 della Policy Cyber Security Aziendale, che viene aggiornato annualmente dall'incaricato o dall'amministratore di sistema, ove presente. Viene predisposto l'aggiornamento automatico dall'antivirus e verificato dall'incaricato. Per minimizzare il rischio da virus informatici, gli utilizzatori dei PC adottano delle specifiche istruzioni presenti nella Cyber Security Aziendale.

Incident management
L'obbiettivo principale del processo di gestione degli incidenti di sicurezza informatica (Incident Management) sono di minimizzare o evitare l'impatto di eventi malevoli, individuare ed attuare tutte le attività di ripristino a seguito di un incidente e adottare le misure idonee per contenere o contrastare l'incidente, infine, di sensibilizzare le tematiche di sicurezza informatica. A tal fine l'agente viene incaricato come responsabile per la gestione delle attività della sicurezza informatica. Qualora venga nominato un incaricato interno o esterno dell'organizzazione per tale scopo si rinvia la nomina al contratto stipulato tra le parti.

Il monitoraggio degli eventi di sicurezza consiste nell'insieme delle attività di controllo finalizzate al rilevamento di eventi con rilevanza nella sicurezza informatica. Tali attività sono svolte dall'incaricato. Le segnalazioni degli eventi possono provenire da diverse fonti:

- Direttamente da parte di un addetto che utilizza i servizi informatici, che può rilevare per esempio un accesso non autorizzato a dati, alterazioni al sito web, indisponibilità di un servizio informatico, ecc. L'addetto quindi è tenuto a comunicare l'evento, in modo verbale o scritto, all'incaricato che provvederà a raccogliere le informazioni e valutare l'eventuale azione al fine di evitare un incidente.

- In modo automatico da sistemi informatici. Alcuni degli strumenti informatici adottati per tali attività: sistemi antivirus (rileva, blocca e traccia il virus); sistemi Antispam (rileva, blocca e segnala la posta elettronica indesiderata); sistemi firewall (rileva, blocca, traccia e segnala l'utilizzo di servizi di rete e/o le richieste di accesso alla rete non conformi);

Gli eventi rilevati durante il monitoraggio vengono analizzati e valutati dall'incaricato al fine di individuare gli interessati all'evento e la criticità dell'evento. Tutte le informazioni, eventuali comunicazioni agli interessati e le attività effettuate vengono tracciate su un apposito supporto (cartaceo o informatico). Dopo aver individuato gli asset interessati dall'evento ed individuato una criticità l'incaricato si affida a terzi tecnicamente qualificati per risolvere l'incidente. Se si verifica un incidente si attueranno delle disposizioni al fine di innalzare il livello di attenzione su determinati scenari di minaccia o particolari aspetti tecnologici e organizzativi.

Decommissioning
In caso di smaltimento di rifiuti elettrici ed elettronici il responsabile per la gestione delle attività di sicurezza informatica, provvede alla distruzione dei supporti. Tale attività consiste nella distruzione fisica o di disintegrazione del supporto al fine di effettuare l'effettiva cancellazione dei dati

personali contenuti nelle apparecchiature elettriche ed elettroniche, in modo da impedire l'acquisizione indebita di dati personali. Tali misure e accorgimenti vengono attuate conferendo incarico a terzi tecnicamente qualificati, quali centri di assistenza, produttori e distributori di apparecchiature che attestino l'esecuzione delle operazioni effettuate o che si impegnino ad effettuarle

11 Valutazione d'impatto sulla protezione dei dati

La valutazione di impatto sulla protezione dei dati (DPIA) è una procedura prevista dall'art. 35 del Regolamento UE 679/2016 che mira a descrivere il trattamento dei dati per valutarne la necessità e la proporzionalità nonché i relativi rischi, allo scopo di approntare misure idonee ad affrontarli. Un DPIA può riguardare un singolo trattamento oppure più trattamenti che presentano analogie in termini di natura, ambito, contesto, finalità e rischi.

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

	PROBABILITA'		
	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.

Categoria di interessati:	**CLIENTI - FORNITORI - DIPENDENTI E COLLABORATORI**
Finalità del trattamento:	ATTIVITA' AMMINISTRATIVE CLIENTI (1 A) ATTIVITA' AMMINISTRATIVE FORNITORI (2 A) ATTIVITA' AMMINISTRATIVE CLIENTI (3 B)

VALUTAZIONE D'IMPATTO

Rischio	Misure di sicurezza	Istruzione	Archivio	Responsabile	Verifica	G	P	R
Distruzione dati	Archivi in armadi protetti da incendi e calamità	Istruzione 01	Archivio amministrativo cartaceo	Incaricato amministrativo	Controllo periodico	M	B	B
Perdita dati	Archivi protetti e chiusi a chiave	Istruzione 01	Archivio amministrativo cartaceo	Incaricato amministrativo	Controllo periodico	M	B	B
Modifica dati	Documenti cartacei non modificabili	Istruzione 01	Archivio amministrativo cartaceo	Incaricato amministrativo	Controllo periodico	B	B	B
Divulgazione non autorizzata dei dati	Documenti in archivio protetto e chiuso a chiave	Istruzione 01	Archivio amministrativo cartaceo	Incaricato amministrativo	Controllo periodico	M	B	B
Accesso accidentale o non autorizzato	Documenti posizione su armadi protetti e chiusi a chiavi	Istruzione 01	Archivio amministrativo cartaceo	Incaricato amministrativo	Controllo periodico	M	B	B

VALUTAZIONE D'IMPATTO - supporti informatici

Rischio	Misure di sicurezza	Documento	Archivio	Responsabile	Verifica	G	P	R
Distruzione dati	Back up esistente	Nomina Responsabile Istruzione 01	-Gestionale amministrativo -Email -Commercialista -Consulente del lavoro	- Commercialista - Consulente del lavoro - Incaricato amministrativo - Amministratore di sistema	Annuale	M	B	B
Perdita dati	Back up esistente	Nomina Responsabile Istruzione 01	-Gestionale amministrativo -Email -Commercialista -Consulente del lavoro	- Commercialista - Consulente del lavoro - Incaricato amministrativo - Amministratore di sistema	Annuale	M	B	B
Modifica dati	Accesso ai dati regolato	Nomina Responsabile Istruzione 01	- Gestionale amministrativo -Email -Commercialista -Consulente del lavoro	- Commercialista - Consulente del lavoro - Incaricato amministrativo - Amministratore di sistema	Annuale	M	B	B
Divulgazione non autorizzata dei dati	Autorizzati al trattamento solo personale identificato	Nomina Responsabile Istruzione 01	- Gestionale amministrativo - Email -Commercialista - Consulente del lavoro	- Commercialista - Consulente del lavoro - Incaricato amministrativo - Amministratore di sistema	Annuale	B	B	B
Accesso accidentale o non autorizzato	Autorizzati al trattamento solo personale identificato	Nomina Responsabile Istruzione 01	- Gestionale amministrativo - Email -Commercialista -Consulente del lavoro	- Commercialista - Consulente del lavoro - Incaricato amministrativo - Amministratore di sistema	Annuale	B	B	B

Categoria di interessati:	**CLIENTI**
Finalità del trattamento:	ANALISI ESIGENZE ASSICURATIVE (1 B)

VALUTAZIONE D'IMPATTO

Rischio	Misure di sicurezza	Istruzione	Archivio	Responsabile	Verifica	G	P	R
Distruzione dati	Archivi in armadi protetti da incendi e calamità	Istruzione 02	Archivio polizze cartaceo	Autorizzati al trattamento	Controllo periodico	M	B	B
Perdita dati	Archivi protetti e chiusi a chiave	Istruzione 02	Archivio polizze cartaceo	Autorizzati al trattamento	Controllo periodico	M	B	B
Modifica dati	Documenti cartacei non modificabili	Istruzione 02	Archivio polizze cartaceo	Autorizzati al trattamento	Controllo periodico	M	B	B
Divulgazione non autorizzata dei dati	Documenti in archivio protetto e chiuso a chiave	Istruzione 02	Archivio polizze cartaceo	Autorizzati al trattamento	Controllo periodico	M	B	B
Accesso accidentale o non autorizzato	Documenti posizione su armadi protetti e chiusi a chiavi	Istruzione 02	Archivio polizze cartaceo	Autorizzati al trattamento	Controllo periodico	M	B	B

VALUTAZIONE D'IMPATTO - supporti informatici

Rischio	Misure di sicurezza	Documento	Archivio	Responsabile	Verifica	G	P	R
Distruzione dati	Back up esistente	Istruzione 02	Archivio polizze digitali scansionate Sistema informatico d'agenzia	- Autorizzati al trattamento - Responsabili esterni al trattamento dati	Annuale	M	B	B
Perdita dati	Back up esistente	Istruzione 02	Archivio polizze digitali scansionate Sistema informatico d'agenzia	- Autorizzati al trattamento - Responsabili esterni al trattamento dati	Annuale	M	B	B
Modifica dati	Accesso ai dati regolato	Istruzione 02	Archivio polizze digitali scansionate Sistema informatico d'agenzia	- Autorizzati al trattamento - Responsabili esterni al trattamento dati	Annuale	M	B	B
Divulgazione non autorizzata dei dati	Autorizzati al trattamento solo personale identificato	Istruzione 02	Archivio polizze digitali scansionate Sistema informatico d'agenzia	- Autorizzati al trattamento - Responsabili esterni al trattamento dati	Annuale	M	B	B
Accesso accidentale o non autorizzato	Autorizzati al trattamento solo personale identificato	Istruzione 02	Archivio polizze digitali scansionate Sistema informatico d'agenzia	- Autorizzati al trattamento - Responsabili esterni al trattamento dati	Annuale	M	B	B

Categoria di interessati:	CLIENTI - DIPENDENTI E COLLABORATORI
Finalità del trattamento:	VIDEOSORVEGLIANZA (1 C - 3 D)

VALUTAZIONE D'IMPATTO - supporti informatici

Rischio	Misure di sicurezza	Documento	Archivio	Responsabile	Verifica	G	P	R
Distruzione dati	Hard disk protetto da incendio	Procedura videosorveglianza Istruzione 05	Hard disk registrazione	Incaricato videosorveglianza	Iniziale e in caso di variazioni	M	B	B
Perdita dati	Hard disk nascosto	Procedura videosorveglianza Istruzione 05	Hard disk registrazione	Incaricato videosorveglianza	Iniziale e in caso di variazioni	M	B	B
Modifica dati	Accesso hard disk solo con chiave	Procedura videosorveglianza Istruzione 05	Hard disk registrazione	Incaricato videosorveglianza	Iniziale e in caso di variazioni	M	B	B
Divulgazione non autorizzata dei dati	Accesso hard disk solo a personale designato	Procedura videosorveglianza Istruzione 05	Hard disk registrazione	Incaricato videosorveglianza	Iniziale e in caso di variazioni	M	B	B
Accesso accidentale o non autorizzato	Accesso hard disk solo a personale designato	Procedura videosorveglianza Istruzione 05	Hard disk registrazione	Incaricato videosorveglianza	Iniziale e in caso di variazioni	M	B	B

Categoria di interessati:	DIPENDENTI E COLLABORATORI
Finalità del trattamento:	RICERCA E GESTIONE DEL PERSONALE (3 A)

VALUTAZIONE D'IMPATTO

Rischio	Misure di sicurezza	Istruzione	Archivio	Responsabile	Verifica	G	P	R
Distruzione dati	Archivi in armadi protetti da incendi e calamità	Istruzione 06	Archivio amministrativo cartaceo Curriculum	Incaricato amministrativo	Controllo periodico	M	B	B
Perdita dati	Archivi protetti e chiusi a chiave	Istruzione 06	Archivio amministrativo cartaceo Curriculum	Incaricato amministrativo	Controllo periodico	M	B	B
Modifica dati	Documenti cartacei non modificabili	Istruzione 06	Archivio amministrativo cartaceo Curriculum	Incaricato amministrativo	Controllo periodico	M	B	B
Divulgazione non autorizzata dei dati	Documenti in archivio protetto e chiuso a chiave	Istruzione 06	Archivio amministrativo cartaceo Curriculum	Incaricato amministrativo	Controllo periodico	M	B	B
Accesso accidentale o non autorizzato	Documenti posizione su armadi protetti e chiusi a chiave	Istruzione 06	Archivio amministrativo cartaceo Curriculum	Incaricato amministrativo	Controllo periodico	M	B	B

VALUTAZIONE D'IMPATTO - supporti informatici

Rischio	Misure di sicurezza	Documento	Archivio	Responsabile	Verifica	G	P	R
Distruzione dati	Back up esistente	- Nomina Responsabile esterno - Istruzione 06	email	- Commercialista - Consulente del lavoro - Incaricato amministrativo	Annuale	B	B	B
Perdita dati	Back up esistente	- Nomina Responsabile esterno - Istruzione 06	email	- Commercialista - Consulente del lavoro - Incaricato amministrativo	Annuale	B	B	B
Modifica dati	Accesso ai dati regolato	- Nomina Responsabile esterno - Istruzione 06	email	- Commercialista - Consulente del lavoro - Incaricato amministrativo	Annuale	B	B	B
Divulgazione non autorizzata dei dati	Autorizzati al trattamento solo personale identificato	- Nomina Responsabile esterno - Istruzione 06	email	- Commercialista - Consulente del lavoro - Incaricato amministrativo	Annuale	B	B	B
Accesso accidentale o non autorizzato	Autorizzati al trattamento solo personale identificato	- Nomina Responsabile esterno - Istruzione 06	email	- Commercialista - Consulente del lavoro - Incaricato amministrativo	Annuale	B	B	B

Categoria di interessati:	DIPENDENTI E COLLABORATORI
Finalità del trattamento:	SUPPORTO ATTIVITA' DI MARKETING (3 C)

VALUTAZIONE D'IMPATTO

Rischio	Misure di sicurezza	Istruzione	Archivio	Responsabile	Verifica	G	P	R
Distruzione dati	Archivi in armadi protetti da incendi e calamità	Istruzione 03	Depliant commerciali	Incaricato amministrativo	Controllo periodico	M	B	B

Perdita dati	Archivi protetti e chiusi a chiave	Istruzione 03	Depliant commerciali	Incaricato amministrativo	Controllo periodico	M	B	B
Modifica dati	Documenti cartacei non modificabili	Istruzione 03	Depliant commerciali	Incaricato amministrativo	Controllo periodico	M	B	B
Divulgazione non autorizzata dei dati	Documenti in archivio protetto e chiuso a chiave	Istruzione 03	Depliant commerciali	Incaricato amministrativo	Controllo periodico	M	B	B
Accesso accidentale o non autorizzato	Documenti posizione su armadi protetti e chiusi a chiavi	Istruzione 03	Depliant commerciali	Incaricato amministrativo	Controllo periodico	M	B	B

VALUTAZIONE D'IMPATTO - supporti informatici

Rischio	Misure di sicurezza	Documento	Archivio	Responsabile	Verifica	G	P	R
Distruzione dati	Back up esistente	Nomina Responsabile esterno Istruzione 03	Sito internet	Incaricato amministrativo	Annuale	B	B	B
Perdita dati	Back up esistente	Nomina Responsabile esterno Istruzione 03	Sito internet	Incaricato amministrativo	Annuale	B	B	B
Modifica dati	Accesso ai dati regolato	Nomina Responsabile esterno Istruzione 03	Sito internet	Incaricato amministrativo	Annuale	B	B	B
Divulgazione non autorizzata dei dati	Autorizzati al trattamento solo personale identificato	Nomina Responsabile esterno Istruzione 03	Sito internet	Incaricato amministrativo	Annuale	B	B	B
Accesso accidentale o non autorizzato	Autorizzati al trattamento solo personale identificato	Nomina Responsabile esterno Istruzione 03	Sito internet	Incaricato amministrativo	Annuale	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 esigenze assicurative	BASSO	BASSO	BASSO	BASSO	BASSO
1 C	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 E COLLABORATORI				
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

12 Verifica rispetto requisiti minimi di sicurezza

12.1 Descrizione struttura archivi

Elenco attrezzature informatiche:
Personal computer di proprietà dell'agenzia o di collaboratore.
L'amministratore di sistema provvede a compilare e tenere aggiornato l'allegato 1 Policy Cyber Security Aziendale, comprensivo dei controlli in materia, indicando, in particolare i sistemi operativi e l'antivirus in uso.

Elenco archivi cartacei:
- Archivio amministrativo
- Elenco pratiche intermediazione assicurativa
- Archivio schede clienti

Elenco archivi informatici:
Sistema informatico amministrativo: SAVE S.RL.
Sistema informatico CRM: ASSIEASY

12.2 Protezione dati personali in formato elettronico

Sono adottati i seguenti accorgimenti minimi:

Report annuale - Allegato 1 policy cyber security aziendale
L'amministratore di sistema provvede a compilare e tenere aggiornato l'allegato 1 Policy Cyber Security Aziendale, comprensivo dei controlli in materia, indicando, in particolare i sistemi operativi e l'antivirus in uso, nonchè i software di gestione in uso.
Gestione configurazione
La configurazione standard dei dispositivi è svolta dall'Amministratore di Sistema, con account dedicato.
Analisi della vulnerabilità
Periodicamente, l'Amministratore di sistema provvede ad analizzare la vulnerabilità dei sistemi ed attuare azioni a protezione della rete.
Privilegi di Amministratore
L'accesso ai PC da parte dell'Amministratore di Sistema è svolto con account dedicata.
Gli utenti, con le loro credenziali, non possono svolgere attività riservate all'Amministratore.
Antivirus e malware
Tutti i PC sono dotati di sistema di protezione antivirus, come indicato nei report di controllo predisposti dall'Amministratore.
Back up
Viene eseguito un back up periodico verificando idonea configurazione, protezione e ripristino dati. Viene conservato su su disco esterno
Sistema di autenticazione informatica
I personal computer sono protetti da una password richiesta per ogni utente.
Inoltre, 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 annuale.
Sistemi di autorizzazione
Tutti gli utenti (dipendenti e collaboratori) hanno lo stesso livello di autorizzazione.

Non è quindi necessario conservare le credenziali di accesso in busta chiusa.
L'amministratore di sistema provvede a resettare le password eventualmente perse.

Copie di salvataggio automatico dei dati

Con frequenza settimanale viene eseguita la copia di back-up. Le copie di back-up sono opportunamente conservate.

Sistemi per la protezione contro elementi esterni

I dispositivi sono protetti da firewall di rete.

Protezione del server

Il server è posizionato all'interno dei locali agenziali, con adeguati sistemi di protezione per consentirne l'accesso solo all'Amministratore di Sistema.

12.3 Protezione dati personali in formato cartaceo

I documenti cartacei contenenti dati identificativi di clienti, fornitori e dipendenti sono controllati e custoditi in armadio chiuso a chiave in modo da essere utilizzati solo dal personale incaricato 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.

12.4 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 e il telefax sono posizionati in modo da non consentire ad estranei la lettura o la sottrazione dei documenti;
- gli addetti esterni alle pulizie svolgono le operazioni in orari di lavoro oppure al di fuori dell'orario lavorativo i documenti cartacei contenenti dati personali sono custoditi in armadi chiusi a chiave.
- 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.

12.5 Criteri e modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento (DISASTE RECOVERY)

Il Server è fisicamente presente in locale protetto e con accesso consentito solo all'Amministratore di Sistema; il backup viene eseguito giornalmente su cassette di registrazione esterne settimanali, custodite poi all'interno di apposito contenitore ignifugo e chiuso a chiave.
In caso di perdita dei dati o malfunzionamenti server, l'Amministratore di sistema provvede a ripristinare un nuovo server e caricare l'ultimo back up eseguito.

13 Verifiche periodiche

Controllo gestionale:
Il presente registro viene modificato al mutare degli elementi contenuti tenendo conto delle modalità e le tipologie del trattamento con cadenza almeno biennale.
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 della società esterna:

K Partners Srl
Sede legale:
Piazza della Repubblica, 32Milano (MI)
e-mail: assistenza@kpartners.it

Referente: ing. Francesco Netti

La società provvede con frequenza almeno annuale a svolgere audit interni, elaborando una relazione finale di audit che identifica il livello di sicurezza presente.
Le registrazioni di tali verifiche sono opportunamente conservate.

Controllo misure di sicurezza informatiche:
È presente un report annuale compilato dall'amministratore di sistema sul grado di applicazione delle misure minime di sicurezza. I requisiti di un sistema di sicurezza informatico sono volti all'integrità, alla riservatezza e alla disponibilità dei dati memorizzati tramite strumenti elettronici.

14 Violazione dei dati personali (Data Breach)

Una 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.
Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali. Alcuni possibili esempi:
- l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati;
- il furto o la perdita di dispositivi informatici contenenti dati personali;
- la deliberata alterazione di dati personali;
- l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.;
- la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;
- la divulgazione non autorizzata dei dati personali.

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 ingiustificato 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 comporti un rischio per i diritti e le libertà delle persone fisiche.
La notifica deve contenere le informazioni previste all'art. 33, par. 3 del Regolamento (UE) 2016/679 e indicate nell'allegato al Provvedimento del Garante del 30 luglio 2019 sulla notifica delle violazioni dei dati personali (doc. web n. 9126951).
Qualora si utilizzi per la notifica il modello allegato al provvedimento, è necessario scaricarlo sul proprio dispositivo e successivamente procedere alla sua compilazione. (Allegato 39)

Comunicazione all’interessato

Quando la violazione dei dati personali comporta un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all’interessato senza giustificato ritardo, utilizzando i canali più idonei, a meno che abbia già preso misure tali da ridurne l’impatto.
Inoltre, a prescindere dalla notifica all’autorità di controllo competente, il Titolare del trattamento predispone un apposito registro, documentando le violazioni dei dati personali nell'**allegato 40** “*Registro delle Violazioni dei dati*”.

Tipologie di violazione di dati personali

Vanno notificate unicamente le violazioni di dati personali che possono avere effetti avversi significativi sugli individui, causando danni fisici, materiali o immateriali.
Ciò può includere, ad esempio, la perdita del controllo sui propri dati personali, la limitazione di alcuni diritti, la discriminazione, il furto d'identità o il rischio di frode, la perdita di riservatezza dei dati personali protetti dal segreto professionale, una perdita finanziaria, un danno alla reputazione e qualsiasi altro significativo svantaggio economico o sociale.

15 ALLEGATI:

Documento Elenco incaricati al trattamento (struttura organizzativa)
Documento Responsabilità referente privacy

Allegato 1: Nomina di persona autorizzata al trattamento dati personali
Allegato 2: Nomina responsabile esterno trattamento dati
Allegato 3: Informativa privacy dipendenti e collaboratori
Allegato 4: Regolamento Aziendale

IN CASO DI PRESENZA DEL SITO INTERNET:
Allegato 21: Informativa sui Cookies
Allegato 22a: Informativa privacy solo servizio
Allegato 22b: Informativa privacy con marketing
Allegato 23: Istruzioni per flag consensi
Allegato 24: Informativa per inserimento Curriculum
Allegato 25: Informativa collaboratori

IN CASO DI PRESENZA DI VIDEOSORVEGLIANZA:
Allegato 31: Informativa dipendenti installazione videosorveglianza
Allegato 32: Incarico per Designato alla videosorveglianza
Allegato 33: Domanda Ispettorato del Lavoro
Allegato 34: Avviso attivazione videosorveglianza
Allegato 35: Segnare area videosorvegliata
Allegato 36: Informativa nuovi dipendenti videosorveglianza attivata

Allegato 39: Modulo notifica violazione dei dati
Allegato 40: Registro delle violazioni dei dati.
Allegato 50: Cartello area riservata