Modello Organizzativo Privacy (M.O.P.)

C.S.U. G. Zorzetto
CONSORZIO SOCIALE UNITARIO G. ZORZETTO

con sede legale e operativa per il trattamento dei dati in
Via Asseggiano 41/N - 30174 Venezia Mestre,
Part. IVA 02894130273, n. REA: VE – 246451,
in persona del legale rappresentante *pro tempore*.

Sommario

1. PRESENTAZIONE MODELLO ORGANIZZATIVO PRIVACY

Il Modello Organizzativo Privacy (MOP) è uno strumento che definisce le misure e le procedure adottate da un'organizzazione per garantire la protezione dei dati personali, conformemente al Regolamento Generale sulla Protezione dei Dati (GDPR). Serve a documentare le attività svolte per adempiere agli obblighi previsti dalla normativa, assicurando la corretta gestione dei dati e la loro sicurezza.
Il MOP è uno strumento fondamentale per dimostrare la conformità al GDPR e alle normative sulla protezione dei dati.

- **Aiuta** a identificare e gestire i rischi legati al trattamento dei dati personali, riducendo la probabilità di violazioni.
- **Consente** all'organizzazione di dimostrare di aver adottato tutte le misure necessarie per proteggere i dati personali, promuovendo un approccio responsabile.
- **Contribuisce** a garantire la trasparenza nel trattamento dei dati, informando gli interessati sulle modalità di gestione dei loro dati.
- **Fornisce** un quadro di riferimento per migliorare costantemente le pratiche di protezione dei dati all'interno dell'organizzazione.

Modello Organizzativo Privacy è uno strumento strategico per le organizzazioni che vogliono gestire efficacemente la protezione dei dati personali, garantendo la conformità normativa e promuovendo una cultura della privacy.

IL TITOLARE DEL TRATTAMENTO DEI DATI ovvero il **CONSORZIO SOCIALE UNITARIO "G. ZORZETTO" Società Cooperativa Sociale,** (di seguito denominato "CSU Zorzetto") intende dotarsi di linee guida che consentano di affrontare in maniera organica gli obblighi normativi in materia di protezione dei dati personali, così da conseguire i migliori risultati nel proteggere le informazioni e i dati gestiti nell'ambito delle proprie attività da tutte le minacce interne o esterne, intenzionali o accidentali, secondo le disposizioni previste dalla normativa comunitaria e nazionale delegando la gestione a terzi.

Dato che il rispetto di tali principi è responsabilità del Titolare del trattamento che, supportato dalle figure preposte, comporta una valutazione, una gestione e un monitoraggio continuo del rischio con il compito di far rispettare la presente Policy nella propria area funzionale di responsabilità.
Tutti gli incaricati, nessuno escluso, sono responsabili del rispetto dei principi e delle regole definite nel presente documento. L'osservanza delle disposizioni della presente Policy deve considerarsi parte essenziale delle obbligazioni contrattuali dei soci, dipendenti e collaboratori.

In ragione delle proprie competenze professionali e dei poteri gerarchici e funzionali adeguati alla natura dell'incarico conferito, tutte le figure preposte hanno il compito di garantire e vigilare sull'attuazione delle misure tecniche, organizzative e di sistema, nonché di supervisionare, anche sulla base delle direttive generali impartite dal Titolare o dal Responsabile del Trattamento, lo svolgimento delle operazioni di trattamento effettuate.

Lo scopo del presente documento e di quelli ad esso collegati è definire il **Modello Organizzativo Privacy (*Policy Privacy*)**, ovvero individuare strategia, linee guida generali e disposizioni operative interne volte a disciplinare il trattamento dei dati personali.

Per raggiungere gli obiettivi sopra definiti, il CSU ZORZETTO adotta misure organizzative per essere in grado di dimostrare in ogni momento il rispetto delle norme in materia e, in particolare dei seguenti principi fondamentali:

1. **liceità, correttezza e trasparenza** - i dati personali sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
2. **limitazione della finalità** - raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;
3. minimizzazione dei dati - adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
4. **esattezza** - esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
5. **limitazione della conservazione** - conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato;
6. **integrità e riservatezza** - trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

L'osservanza di tali principi è assicurata dai responsabili che svolgono le funzioni di titolare, per competenza, con l'adozione di misure tecniche e organizzative adeguate atte a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente alla normativa sin dalla progettazione e con misure di protezione per impostazione predefinita nonché per gestire in maniera trasparente il rapporto con gli interessati mettendoli in condizione di esercitare i propri diritti in maniera rapida ed efficace.

Il **Modello Organizzativo Privacy** definisce le "Linee Guida" e i "Principi Fondamentali" di organizzazione e di gestione volti a un corretto governo dei trattamenti dei Dati Personali, in linea con gli adempimenti richiesti dalla normativa vigente. Contestualmente, le **Procedure interne** definiscono regole, attività e relativi ruoli e responsabilità per la gestione di processi per la gestione dei dati personali. I **Documenti** rappresentano lo strumento di supporto di riferimento per la gestione e l'aggiornamento degli adempimenti per la protezione dei dati (es. modelli di informative e consenso, nomine, accordi contrattuali con le terze parti), documentazione a supporto della protezione dati (Registro dei trattamenti, procedure per la gestione delle violazioni) e materiale formativo.

Nel rispetto del D.Lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" (Codice della Privacy), come modificato dal D.Lgs. 10 agosto 2018, n. 101 e del Regolamento (UE) del Parlamento Europeo e del Consiglio del 27 aprile 2016, n. 679 (*GDPR – General Data Protection Regulamentation*), nonché ulteriori provvedimenti in materia di fonte normativa secondaria in vigore al momento dell'approvazione della seguente *policy*. In essa sono quindi disciplinati i ruoli e le responsabilità nonché gli adempimenti da seguire in materia di protezione dei Dati Personali ai sensi del "Codice della Privacy" e del "GDPR", anche con riferimento alle decisioni e ai provvedimenti emessi dal Garante Europeo della Protezione dei Dati (GEPD) e dall'Autorità Garante Nazionale per la protezione dei dati personali.

2. TITOLARE DEL TRATTAMENTO DEI DATI

Il Titolare del Trattamento definisce e stabilisce, singolarmente o insieme ad altri, le finalità e le modalità del trattamento dei dati personali. Il titolare del trattamento GDPR deve garantire la conformità al Regolamento, tutelando gli interessati, assicurando la sicurezza dei dati, documentando le attività, nominando un responsabile del trattamento, e rispondendo a eventuali violazioni cooperando con le autorità preposte e collaborando con l'autorità di controllo (Garante Privacy) in caso di richieste o indagini.
Questo include il rispetto dei principi di protezione dei dati, la tutela dei diritti degli interessati, la conservazione della documentazione, la notifica delle violazioni dei dati e la scelta di eventuali responsabili del trattamento.

In maniera semplificata deve:

Definire finalità e mezzi: Decidere "perché" (finalità) e "come" (mezzi) i dati personali devono essere trattati, compresi gli aspetti di sicurezza.

Scegliere e gestire i responsabili del trattamento: Se si avvale di terzi per il trattamento dei dati, deve scegliere un responsabile idoneo e stipulare un contratto che ne disciplini il rapporto.

Attivarsi per la Sicurezza dei Dati: Adottare misure tecniche e organizzative adeguate a proteggere i dati personali da distruzione, perdita, alterazione o accesso illecito, garantendo la riservatezza e l'integrità.

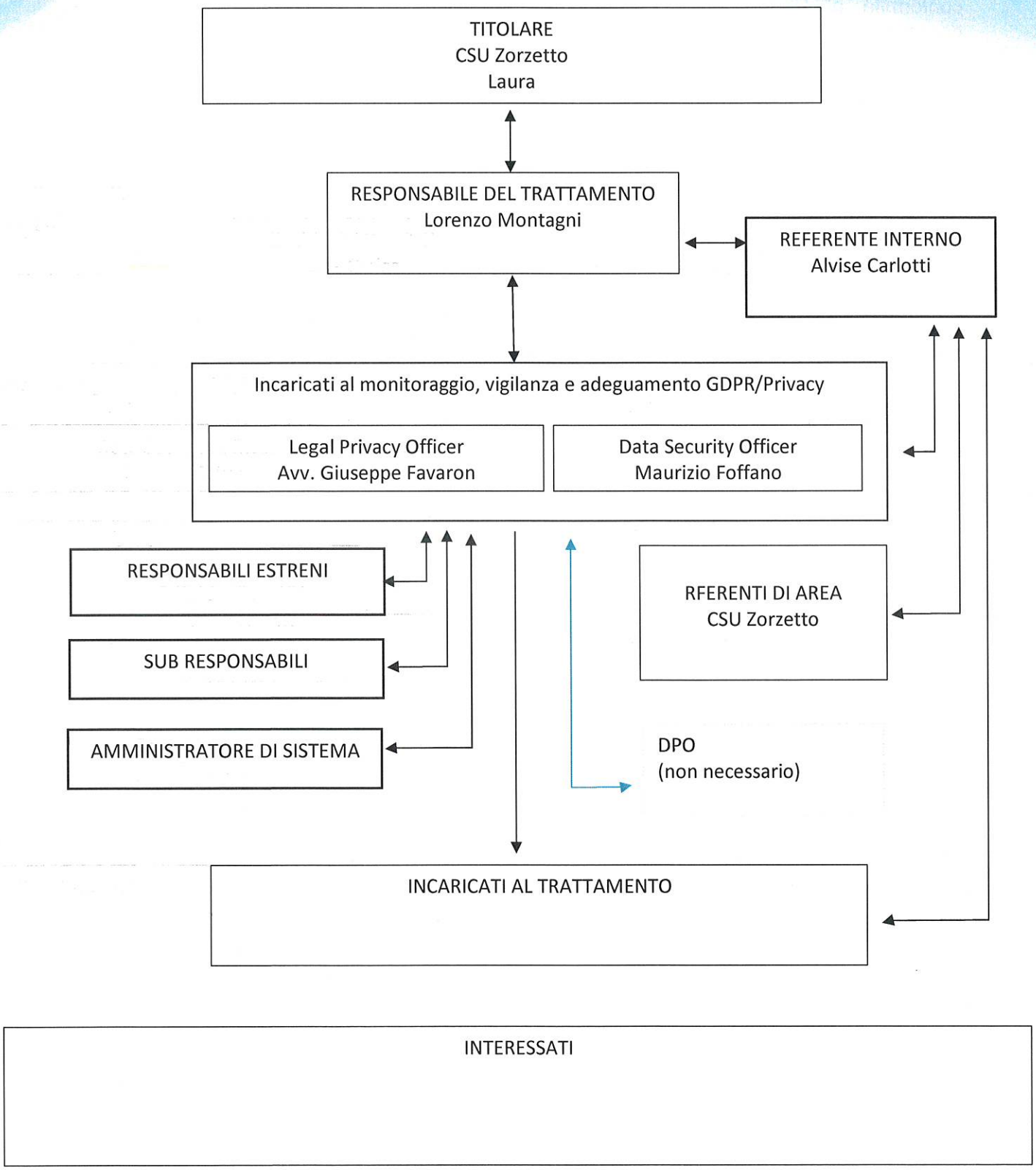
Per CSU Zorzetto, le funzioni di Titolare sono svolte, per competenza, dalle diverse articolazioni interne sulla base dei regolamenti e degli atti di indirizzo strategico che sono stati individuati per i rispettivi ambiti di competenza:

1. Responsabile del Trattamento con funzioni di coordinamento;
2. Incaricati monitoraggio, vigilanza e adeguamento GDPR/Privacy;
3. Referente Interno GDPR Privacy;
4. Responsabili esterni;
5. Sub Responsabili;
6. Amministratore di sistema;
7. Referenti di area;
8. Incaricati al trattamento.

I responsabili del trattamento nelle loro funzioni di coordinamento possono delegare alcune attività specifiche per trattamenti trasversali che coinvolgono diverse unità organizzative.

Diventa fondamentale che tutti i soggetti coinvolti nel trattamento di dati personali devono contribuire alla protezione dei dati personali dando applicazione alle presenti linee guida.

3. ORGANIGRAMMA GDPR PRIVACY



1. RUOLI FUNZIONALI

Tenuto conto dell'attività e dell'assetto di CSU ZORZETTO, sui trattamenti interni, fra consorziati, con Enti e clienti, sui processi organizzativi e sui presidi tecnologici, si è ritenuto che, **in via generale e salvo eccezioni, la Cooperativa necessita di un supporto per la compliance al GDPR/Privacy. Il supporto è la delega di attività e la gestione del MOP.**

Il Delegato del Titolare del trattamento è, pertanto, la persona fisica designata dal Titolare del trattamento e delegata allo svolgimento delle attività utili a garantire il costante e puntuale rispetto delle normative vigenti in materia di trattamento di dati personali, nonché a rappresentarlo nei rapporti con i soggetti interessati e le Autorità e in tutti gli atti e i contratti di nomina di Terze Parti.
Il Delegato del Titolare GDPR è una figura che può essere incaricata dal titolare del trattamento per svolgere specifici compiti in conformità con il Regolamento Generale sulla Protezione dei Dati (GDPR). In sostanza, il titolare può delegare alcune delle sue responsabilità a questa figura, ma rimane sempre responsabile per la conformità complessiva al GDPR.

Alla delega, rilasciata con apposita nomina, deve essere data adeguata pubblicità, anche interna, pertanto:

- valutato il profilo professionale per le conoscenze sia informatiche che giuridiche, con particolare riferimento alla attività di consulenza e formazione maturata nello specifico,
- nota la partecipazione ad eventi formativi in materia di sicurezza, privacy e GDPR con adeguato livello di conoscenza specialistica e delle competenze per tale incarico,
- rilevato che la proposta non si trova in situazioni di conflitto di interesse con la posizione da ricoprire e i compiti e le funzioni da espletare,

In questa sezione vengono identificati i ruoli/funzioni ministeriali individuati per la definizione del modello di gestione dei dati personali. Tali figure assumono un peso rilevante nell'ambito della protezione dei dati personali e del modello organizzativo e di gestione dei dati personali in quanto svolgono un ruolo di facilitazione e monitoraggio dell'implementazione dei requisiti normativi all'interno del CSU ZORZETTO.

per queste motivazioni si istituisce un

Responsabile della Protezione dei Dati (RPD)
Il Responsabile della Protezione dei Dati Personali è un soggetto designato dal Titolare, o dal Responsabile del trattamento, per assolvere a funzioni di controllo, di consulenza sugli obblighi, formative e informative relativamente all'applicazione del RGPD (ove previsto) e della normativa nazionale in materia di trattamento dei dati personali. Coopera con l'Autorità (e proprio per questo, il suo nominativo va notificato al Garante) e costituisce il punto di contatto, anche rispetto agli interessati, per le questioni connesse al trattamento dei dati personali.

Funzioni, compiti e responsabilità del RPD indicati dagli articoli 38 e 39 del RGPD sono:

1. informare e fornire consulenza al Titolare/Responsabile Interno del Trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi previsti dalla normativa in materia;
2. sorvegliare l'osservanza dei requisiti previsti dal RGPD e dalle altre normative in materia di protezione dei Dati Personali;

3. fornire un parere nell'ambito della valutazione d'impatto sulla protezione dei Dati Personali (ove applicabile) e sorvegliarne lo svolgimento;
4. cooperare e fungere da contatto per l'Autorità di protezione dei dati personali per le questioni riferite ai trattamenti;
5. fungere da punto di contatto tra l'Autorità Garante per la protezione dei dati personali ed il Ministero;
6. fungere da punto di contatto per gli Interessati e garantire, in cooperazione con gli Esercenti le funzioni di Titolare, la gestione delle richieste di informazione o l'esercizio dei diritti riconosciuti dal RGPD.

Delegato al Responsabile Trattamento il *Sig. Maurizio Foffano*,

nato a Mirano (VE) il 09/07/1961, C.F. FFFMRZ61L09F241B Titolare della **TECNOSOFT srl** (per semplicità denominata anche come Azienda) con sede in Mirano (VE) 30035- Via Stazione, 80 Ballò di Mirano, P.I. 02701200277; per lo svolgimento delle funzioni (servizio), persona autorizzata al trattamento così come previsto dalla normativa vigente. Autorizzato al trattamento dei dati personali, anche di carattere sensibile, nell'ambito delle funzioni chiamato a svolgere, ed in particolare per i trattamenti di dati personali riguardanti la gestione dei trattamenti discendenti dalla procedura operativa del Modello Operativo Privacy.

Tempo della delega (servizio)

1) Non è prevista la presenza fisica del Delegato presso la sede del Titolare con periodicità prestabilita e carattere continuativo. Tutti i contatti con il medesimo possono avvenire con comunicazione telefonica e/o e-mail, salvo documentata esigenza da verificare in concreto.
2) Le attività saranno di regola prese in carico entro i cinque giorni lavorativi successivi al ricevimento della richiesta fatta pervenire al Delegato a mezzo comunicazione e-mail o dall'accettazione dell'eventuale preventivo di spesa.
3) In caso di violazione di dati personali (data breach) ai sensi dell'articolo 33 del GDPR è garantita l'eventuale assistenza per gli adempimenti necessari, ivi compresa la notifica al Garante e/o la comunicazione agli interessati nei tempi previsti ai costi previsti.
4) In caso di ispezioni presso la sede del Titolare ad opera del Garante ovvero di soggetti dal medesimo delegati, è garantita l'eventuale presenza in loco come anche l'assistenza telefonica dalla richiesta.
5) Nel periodo intercorrente tra 1 ed il 31 di agosto di ciascun anno il termine di cui al precedente comma 2) è sostituito dal termine di giorni dieci;

Obblighi in capo al Titolare

Per il migliore espletamento dell'incarico i referenti dell'Azienda ed il Sig. Maurizio Foffano, congiuntamente ed anche disgiuntamente tra loro, hanno piena facoltà di frequentare gli uffici del Titolare, anche avvalendosi di propri collaboratori, nei tempi e negli orari da concordarsi, in relazione alle necessità di trattazione delle questioni loro affidate.
Il Titolare metterà a disposizione dell'Azienda e del Sig. Maurizio Foffano risorse tecniche e umane idonee allo svolgimento dell'attività concordata.

Durata del contratto

Il rapporto contrattuale avrà decorrenza dalla sua sottoscrizione con validità un anno e verrà rinnovato solo su nuova proposta economica e/o di servizi. Si esclude qualsivoglia forma di rinnovazione tacita.

Il Titolare si riserva la facoltà di disporre il rinnovo del contratto per ulteriori 3(tre) mesi; tempo tecnico ipotizzato come necessario ai fini del subentro del nuovo affidatario. In tali casi l'Azienda ha l'obbligo di continuare a prestare il servizio alle medesime condizioni pattuite con il presente contratto e garantire le caratteristiche tecniche ed il livello offerti. Resta inteso che il rinnovo è in ogni caso subordinato alla previa verifica della sussistenza di idonea copertura finanziaria.

Risoluzione del contratto

Il Titolare si riserva di risolvere anticipatamente il presente contratto in caso di gravi inadempienze da parte dell'Azienda o del Sig. Maurizio Foffano, come ogni azione od omissione che causi gravi danni all'immagine o inadempienze agli obblighi previsti dal presente contratto e dalla normativa citata in premessa.

Eventuali inadempienze agli obblighi previsti nel presente contratto saranno contestate per iscritto concedendo un congruo termine pari, almeno, a trenta (30) giorni, per adempiere agli obblighi contrattuali ovvero per la presentazione di eventuali controdeduzioni. Trascorso tale termine senza che l'Azienda o il Sig. Maurizio Foffano abbiano provveduto ovvero, in caso le controdeduzioni non fossero presentate o risultassero non accoglibili, Il Titolare potrà procedere alla risoluzione del contratto.

Il contratto si risolverà di diritto ai sensi dell'art. 1456 c.c. quando l'inadempienza riguardi una delle seguenti obbligazioni:

a) mancata esecuzione delle obbligazioni di risultato;
b) caso di subappalto non autorizzato;
c) violazione del segreto aziendale e della riservatezza;
d) violazione tutela della proprietà intellettuale.

Responsabilità del delegato:

Le responsabilità del Delegato dipendono dalle specifiche deleghe conferite dal titolare. Queste includono anche:

- Gestione degli accessi ai dati da parte degli interessati.
- Gestione delle notifiche di violazione dei dati.
- Supporto nella valutazione dell'impatto sulla protezione dei dati (DPIA).
- Implementazione delle misure di sicurezza tecniche e organizzative.
- Formazione del personale sul GDPR.

Responsabilità del titolare:

- Il titolare rimane responsabile per la scelta del delegato e per la verifica delle sue competenze.
- La definizione chiara dei compiti e delle responsabilità del delegato.
- La supervisione dell'attività del delegato e la verifica della conformità al GDPR.
- La gestione delle conseguenze di eventuali violazioni dei dati, anche se causate dal delegato.

In sintesi, la delega al trattamento dei dati personali è uno strumento utile per il titolare, ma non lo esonera dalla sua responsabilità di garantire la conformità al GDPR.

Le funzioni e le responsabilità del Responsabile del trattamento, nel contratto o convenzione stipulata prima dell'inizio dei trattamenti e devono sempre comprendere i seguenti compiti:

a) effettuare le operazioni di trattamento dei dati personali messi a disposizione dal Titolare nel pieno rispetto dei principi e delle disposizioni della vigente Normativa in materia di

protezione dei dati personali ed esclusivamente ai fini dell'esecuzione del Contratto, secondo le modalità, procedure e modulistiche nel tempo indicate dal Titolare;

b) trattare i dati personali soltanto sulla base delle documentate istruzioni fornite dal Titolare, anche in caso di eventuale trasferimento di dati personali verso soggetti stabiliti in Paesi al di fuori dell'UE, che potrà essere effettuato solo previa autorizzazione del Titolare medesimo e sulla base delle relative istruzioni, adottando le adeguate garanzie secondo la vigente normativa europea e nazionale di riferimento, garanzie di cui andrà mantenuta adeguata documentazione da fornire, ove richiesto, al Titolare;

c) tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche interessate, adottare misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato ai rischi identificati;

d) curare la predisposizione ed il rispetto delle misure prescritte dall'Autorità Garante per la Protezione dei Dati Personali (in seguito il "Garante"), con il provvedimento del 27 novembre 2008, in merito all'attribuzione delle funzioni di "amministratore di sistema" ed, in particolare, procedere a: (i) conservare direttamente e specificamente gli estremi identificativi delle persone fisiche preposte all'interno della Società quali amministratori del/i sistema/i e, (ii) in tal caso, porre in essere le attività di verifica periodica, con cadenza almeno annuale, sul loro operato, secondo quanto prescritto dal Garante, fino alla eventuale modifica, sostituzione o abrogazione del provvedimento sopra citato, e (iii) rendere disponibile periodicamente e, in ogni caso, almeno annualmente, la lista aggiornata degli amministratori di sistema;

e) prestare nei confronti del Titolare la massima collaborazione necessaria a garantire il rispetto, per quanto di relativa competenza, degli obblighi in tema di violazione dei dati personali, di relativa notifica al Garante e, se del caso, di comunicazione agli interessati;

f) fermo l'obbligo di notificare senza ingiustificato ritardo al Titolare ogni possibile evento qualificabile come violazione dei dati ai sensi dell'articolo 4 n.,12 del RGPD, informare prontamente il Titolare riguardo a qualsiasi ulteriore evento, fatto o circostanza, prevedibile o meno (I.e. incidente di sicurezza), dal quale possa derivare un rischio elevato per i diritti e le libertà fondamentali dei dati personali degli interessati coinvolti nelle operazioni di trattamento;

g) collaborare con il Titolare nell'assolvimento dell'obbligo di eseguire, in tutti i casi in cui ciò sia necessario, idonea valutazione di impatto sulla protezione dei dati, oltre che ai fini dello svolgimento delle procedure di consultazione preventiva con il Garante o le altre autorità competenti, quando richiesto;

h) individuare le persone autorizzate al trattamento dei dati personali che operano sotto la propria autorità (in seguito, gli "Autorizzati al Trattamento/Incaricati") ed adottare le misure necessarie a

    a. garantire l'assunzione da parte di questi ultimi di idonei obblighi di riservatezza in ordine ai dati personali trattati,
    b. fornire loro per iscritto adeguate istruzioni circa il rispetto, in particolare, delle misure per la sicurezza dei dati
    c. vigilare sulla osservanza, da parte degli Autorizzati al Trattamento/Incaricati, delle istruzioni impartite e, più in generale, delle ulteriori vigenti disposizioni di legge,
    d. controllare e riesaminare, almeno annualmente, i privilegi di accesso ai dati da parte degli Autorizzati al Trattamento/Incaricati (fermo restando la tempestività richiesta dalla cessazione di eventuali rapporti di dipendenza e/o collaborazione);

i) assicurare il costante monitoraggio degli adempimenti e delle attività effettuate da chi opera sotto la propria autorità;

j) informare periodicamente il Titolare, su richiesta di quest'ultimo, in ordine all'attività svolta, sia sotto il profilo del trattamento, sia sotto il profilo della sicurezza dei dati;
k) conservare i dati in una forma che consenta l'identificazione degli interessati per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti e successivamente trattati;
l) inviare al Titolare, previa apposita richiesta scritta, al momento della cessazione delle operazioni di trattamento o anche antecedentemente in caso di specifica richiesta del Titolare, la documentazione comprovante l'avvenuta implementazione degli adempimenti privacy;
m) informare prontamente il Titolare di ogni questione rilevante in relazione al ruolo di Responsabile del trattamento, quali a titolo indicativo:
    a. istanze di interessati;
    b. richieste del Garante;
    c. violazioni o messa in pericolo della riservatezza, della completezza o dell'integrità dei dati personali;
n) adottare misure tecniche ed organizzative idonee a poter assistere il Titolare nell'assolvimento del proprio obbligo di fornire adeguato riscontro alle richieste di esercizio dei diritti avanzate da parte degli interessati.
o) comunicare al Titolare qualsiasi richiesta di esercizio di diritti che il Responsabile dovesse ricevere da parte degli interessati, entro un termine massimo di 24 ore dal ricevimento della stessa;
p) non comunicare a terzi e, più in generale, non diffondere i dati ricevuti, se non in presenza di espressa autorizzazione da parte del Titolare e di adeguati presupposti di liceità per tali ulteriori trattamenti;
q) prestare nei confronti del Titolare ogni necessaria collaborazione nell'assolvimento di richieste che dovessero pervenire dal Garante o da altre autorità competenti, o in relazione a procedure o ispezioni che dovessero essere avviate nei confronti del Titolare, nonché in caso di controversie avente ad oggetto la normativa a tutela dei dati personali, dando immediata esecuzione alle istruzioni ricevute e fornendo copia di ogni documento richiesto;
r) consentire l'esecuzione di ogni altra operazione richiesta o necessaria per ottemperare agli obblighi derivanti dalla normativa in materia di protezione dei dati personali di volta in volta applicabile;
s) mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente accordo ed alla vigente Normativa privacy, nonché consentire e contribuire alle attività di revisione, compresi gli audit, che il Titolare (con preavviso minimo di 5 giorni) potrà effettuare, direttamente o avvalendosi di terzi.
t) L'Esercente le funzioni di Titolare provvede a formalizzare, ai sensi dell'art. 28 del RGPD, le suddette responsabilità stipulando e manutenendo specifici accordi di nomina nell'ambito di contratti o convenzioni con i Responsabili del trattamento dei dati personali.
u) Il Responsabile del trattamento, in base agli accordi contrattuali o dietro specifica autorizzazione del Titolare rilasciata dall'Esercente le funzioni di Titolare, può nominare a sua volta soggetti terzi che effettuino trattamenti di dati personali nell'ambito delle attività per le quali è nominato Responsabile quale sub Responsabile. Il Responsabile (Sub Responsabile Esterno del Trattamento) così designato è tenuto a rispettare gli stessi obblighi stabiliti nel contratto stipulato tra il Titolare e il primo Responsabile, che rimane pienamente responsabile per il rispetto degli obblighi da parte del Sub Responsabile.

2. OBIETTIVI GENERALI

Presso la sede legale sono effettivamente svolti e condivisi i principi e le regole da seguire, quando vengono trattati dati personali, indipendentemente dal fatto che i dati siano trattati presso quella sede. In particolare, le Cooperative Consorziate possono trattare i dati personali in qualità di Titolari del trattamento ovvero di Responsabili del trattamento sulla base di appositi accordi sull'argomento volti a disciplinare, nell'ambito dei **rapporti infragruppo,** la natura, la finalità, la durata del trattamento, il tipo di dati personali, le categorie di interessati, gli obblighi e i diritti delle parti.

Per facilitare l'interazione tra le parti, all'interno di ciascuna Consociata dovrà essere individuato un referente o un responsabile per la gestione di tutte le tematiche e le specificità inerenti al trattamento di dati personali. Tale figura dovrà essere individuata dal Titolare di ciascuna Consociata, con i seguenti compiti:

- aggiornare tempestivamente il proprio Titolare e/o i Titolari su eventuali problematiche, inerenti alla protezione dei dati personali, sorte all'interno della Consociata in cui opera, quali ad esempio:
    - divulgazione di dati sensibili a persone on autorizzate;
    - possibile Data Breach;
    - distruzione o perdita, anche accidentale, dei dati personali;
    - accesso non autorizzato ai dati personali;
    - nuovi progetti o trattamenti con impatti GDPR / Privacy;
    - problematiche nella gestione dei diritti degli Interessati;
    - nuove Terze Parti coinvolte nel trattamento di dati personali.
        - supportare i Referenti Interni della Società nell'analisi del rischio;
        - alimentare ed aggiornare periodicamente il Registro dei Trattamenti in collaborazione con i Referenti Interni.

I Referenti Interni sono i soggetti che, responsabili di strutture organizzative aziendali, rappresentano le figure chiave nel trattamento dei dati personali.

Ciascun Referente Interno, in ragione delle proprie competenze professionali e dei poteri gerarchici e funzionali adeguati alla natura dell'incarico conferito, ha il compito di garantire e vigilare sull'attuazione delle misure tecniche, organizzative e di sistema, nonché di supervisionare, anche sulla base delle direttive generali impartite dal Titolare, lo svolgimento delle operazioni di trattamento effettuate dagli Incaricati che operano nell'ambito della struttura organizzativa di cui è responsabile.

Si indicano qui di seguito i principali ambiti di intervento del Referente Interno:

- collaborare con il Titolare nell'esecuzione degli adempimenti previsti dalla normativa;
- dare attuazione ai principi di "Privacy by Design" e "Privacy by Default" secondo quanto previsto dal Modello Organizzativo Privacy, coinvolgendo tempestivamente i referenti, nelle ipotesi di nuovi trattamenti o nuove modalità di svolgimento di trattamenti preesistenti;
- identificare, nell'ambito della propria funzione, le persone autorizzate al trattamento dei dati personali ("Autorizzati del trattamento"), elaborando e fornendo apposite istruzioni scritte per il trattamento dei dati nell'area di appartenenza;
- supervisionare le operazioni di trattamento svolte dai soggetti autorizzati nella funzione di appartenenza, verificando che vengano eseguite in conformità alle istruzioni impartite;

- monitorare l'applicazione dei processi interni previsti al fine di identificare i trattamenti (nuovi e preesistenti) e verificare il rispetto dei tempi di conservazione dei dati personali definiti dal Titolare, garantendo, qualora previsto, che cancellazione e/o anonimizzazione dei dati avvengano in modo conforme alle prescrizioni impartite;
- con riferimento al trattamento dei dati effettuato all'interno della funzione di competenza, alimentare ed aggiornare periodicamente il Registro dei Trattamenti;
- contattare/coinvolgere tempestivamente il DPO ove presente, nel caso di richieste e/o reclami di terzi inerenti alla protezione dei dati personali;
- supportare l'eventuale DPO ed il Titolare nella rilevazione e gestione di potenziali violazioni dei dati personali (Data Breach), garantendo la necessaria collaborazione nelle attività di recovery che dovessero essere individuate (investigazione, mitigazione ed eliminazione delle conseguenze derivanti dalla violazione) e di aggiornamento del Registro delle violazioni.

3. DEFINIZIONI

Ai fini del presente Modello Organizzativo Privacy si applicano le seguenti definizioni, coerenti con quanto previsto dalla normativa di settore:

- **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);
- **Normativa:** D.Lgs. 2003/196 (come modificato dal D.Lgs. 2018/101) e Regolamento (UE) 2016/679, nonché ulteriori provvedimenti in materia di fonte normativa secondaria in vigore al momento dell'approvazione del presente Modello Organizzativo Privacy.
- **Codice Privacy**: Decreto legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" come modificato dal Decreto Legislativo 10 agosto 2018, n. 101;
- **Affiliate**: società controllate o collegate al Titolare del trattamento dei dati stabilite nel territorio dello Stato italiano o in un luogo comunque soggetto alla sovranità dello Stato italiano;
- **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;

- **Dati genetici**: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
- **Dati biometrici**: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
- **Dati relativi alla salute**: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
- **Interessato:** la persona fisica cui si riferiscono i dati personali;
- **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;
- **Titolare del trattamento**: la persona fisica preposta alla sorveglianza sull'applicazione e il rispetto delle disposizioni in materia di trattamento di dati impartite dal Titolare del trattamento e, per quanto di sua competenza se nominato da quest'ultimo, dal DPO;
- **Incaricati**: le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal Responsabile con compiti di coordinamento di più o soggetti autorizzati (o *designati)*;
- **Autorizzato**: le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare del trattamento o dal Responsabile del trattamento (anche soggetti *designati*);
- **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;
- **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;
- **Trattamento transfrontaliero**:
  a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure
  b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente inciderebbe in modo sostanziale sugli interessati in più di uno Stato membro.
- **Paesi terzi**: paesi non appartenenti all'UE o allo spazio Economico Europeo (Norvegia, Islanda, Liechtenstein);

4. AMBITO DI APPLICAZIONE

La politica della privacy (***policy***) e della sicurezza dei trattamenti, che ha scaturito la dotazione del presente **Modello Organizzativo Privacy (M.O.P.)** si applica all'azienda nella sua interezza, a tutti gli organi e alle strutture di qualsiasi livello organizzativo o funzionale.

La sua attuazione è obbligatoria per tutto il personale e deve essere inserita come parte integrante nella regolamentazione di qualsiasi accordo con tutti i soggetti esterni coinvolti con il trattamento di informazioni che rientrano nell'ambito operativo.

CSU Zorzetto consente la comunicazione e la diffusione delle informazioni di tipo procedurale e organizzativo verso l'esterno esclusivamente per il corretto svolgimento delle attività aziendali che avvengono nel rispetto delle regole e delle norme vigenti.

Lo stesso si impegna a garantire e dimostrare che il trattamento dei dati personali avviene in maniera conforme a quanto previsto dalla normativa e, secondo i seguenti principi di liceità, questi sono:

- **trattati in modo lecito**, corretto e trasparente nei confronti dell'interessato;
- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;
- **adeguati, pertinenti e limitati** a quanto necessario rispetto alle finalità per le quali sono trattati;
- **esatti e, se necessario, aggiornati**; a tal proposito sono state adottate misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
- **conservati** in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;
- **trattati in maniera da garantire un'adeguata sicurezza** dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

Le presenti indicazioni sono valide, oltre che per i trattamenti dei dati personali di cui è Titolare, anche per tutti quei trattamenti di cui è nominato Responsabile del trattamento da altri Titolari del trattamento, salvo la presenza di misure più restrittive in materia di protezione dei dati personali contenute nei documenti che regolano i rapporti con il Titolare del trattamento.

Poiché analoghe garanzie di protezione e l'adozione di adeguate misure di sicurezza sono richieste ai soggetti terzi ai quali CSU Zorzetto affida l'incarico di Responsabile del trattamento, la *policy* in oggetto è resa disponibile presso tali Responsabili del trattamento.

5. SICUREZZA DELLE INFORMAZIONI

Il patrimonio informativo da tutelare è costituito dall'insieme delle informazioni trattate nell'espletamento delle procedure aziendali, rispetto alle quali CSU Zorzetto assicura l'integrità e la protezione e consente l'accesso esclusivamente ai ruoli e alle funzioni necessarie e preventivamente autorizzate.

La mancanza di adeguati livelli di sicurezza può infatti comportare il danneggiamento dell'immagine aziendale, la mancata soddisfazione della clientela, il rischio di incorrere in sanzioni legate alla violazione delle leggi vigenti nonché altri danni di natura economica e finanziaria.

Per conseguire sempre l'allineamento normativo e aumentare la capacità di controllo CSU Zorzetto ha istituito e mantiene aggiornato un registro delle attività di trattamento.

CSU Zorzetto identifica, quando ritenuto necessario a seguito delle risultanze dell'analisi dei rischi connessi al trattamento dei dati personali, le ulteriori esigenze di sicurezza tramite la valutazione di impatto sulla protezione dei dati che consente di acquisire un livello aggiuntivo di consapevolezza sul livello di esposizione a minacce dei propri sistemi di gestione dei dati.

La valutazione del rischio, eseguita su tutti i trattamenti in essere o previsti, permette di valutare le potenziali conseguenze e i danni che possono derivare dalla mancata applicazione delle misure di sicurezza al sistema informativo e in generale all'intera organizzazione oltre a indicare quale sia la probabilità che le minacce identificate trovino reale attuazione. I risultati di questa valutazione determinano le azioni necessarie per individuare le corrette e adeguate misure di sicurezza e i meccanismi per garantire la protezione dei dati personali.

La gestione della sicurezza delle informazioni è fondata su alcuni imprescindibili principi generali, di seguito enunciati:

- Esiste un asset aziendale rilevante ai fini della gestione delle informazioni, dove per ciascun argomento è individuato un responsabile (contratti, appalti, incarichi, gestione amministrativa, ecc.);
- Le informazioni sono classificate in base al loro livello di criticità, in modo da essere gestite con livelli di riservatezza, integrità e disponibilità coerenti e appropriati;
- Gli accessi ai sistemi informativi sono sottoposti a una procedura di identificazione e autenticazione. Inoltre, le autorizzazioni di accesso alle informazioni sono differenziate in base al ruolo e agli incarichi ricoperti dai singoli individui, in modo che ogni utente possa accedere alle sole informazioni di cui necessita, e tali autorizzazioni sono periodicamente sottoposte a revisione (come previsto dal Regolamento Informatico);
- Sono definite delle procedure per l'utilizzo sicuro dei beni (luoghi, mezzi di trasporto, strumenti) e delle informazioni aziendali;
- È incoraggiata la piena consapevolezza da parte del personale delle problematiche relative alla sicurezza delle informazioni;
- Per poter prevenire o almeno gestire in modo tempestivo gli incidenti, tutti sono chiamati a rendersi partecipi del sistema di sicurezza aziendale e pertanto devono notificare qualsiasi problema relativo alla sicurezza di cui sono a conoscenza;
- È necessario prevenire l'accesso non autorizzato ai locali e alle apparecchiature dove sono gestite le informazioni;
- È assicurata la conformità con i requisiti legali e con i principi legati alla sicurezza delle informazioni nei contratti con le terze parti;
- È predisposto un piano di continuità che permette all'azienda di affrontare efficacemente un evento imprevisto, garantendo il ripristino dei servizi critici in tempi e con modalità che limitino le conseguenze negative sulla missione aziendale. Gli aspetti di sicurezza sono inclusi in tutte le fasi di progettazione, sviluppo, esercizio, manutenzione, assistenza e dismissione dei sistemi e dei servizi informatici;

- Sono garantiti il rispetto delle disposizioni di legge, di statuti, regolamenti o obblighi contrattuali e di ogni requisito inerente alla sicurezza delle informazioni, riducendo al minimo il rischio di sanzioni legali o amministrative, di perdite rilevanti o danni alla reputazione.

6. RISERVATEZZA DELLE INFORMAZIONI

CSU Zorzetto si impegna a garantire la riservatezza e la confidenzialità delle informazioni e dei dati degli interessati acquisiti nel corso della propria attività in conformità alle procedure interne previste, coerenti con il presente Modello Organizzativo Privacy.

Il trattamento dei dati può essere effettuato attraverso strumenti manuali, informatici e telematici atti a memorizzare, elaborare, gestire e trasmettere i dati stessi nel rispetto delle misure di sicurezza previste. Tutti i soggetti in qualsiasi modo coinvolti nel trattamento dei dati personali, indipendentemente dal rispetto degli obblighi derivanti dal codice deontologico relativo alla professione regolamentata eventualmente esercitata nell'espletamento delle proprie mansioni, sono tenuti al segreto previsto dall'art. 2407 del Codice civile.

CSU Zorzetto si impegna a garantire adeguati livelli minimi di sicurezza delle informazioni rese disponibili da terzi con la medesima diligenza e livello di protezione utilizzati per la sicurezza e la riservatezza dei propri dati.

7. ATTUAZIONE DELLA *POLICY PRIVACY*

L'osservanza e l'attuazione della politica della *policy* privacy che delinea il presente Modello Organizzativo Privacy sono responsabilità di:

- tutto il personale che, a qualsiasi titolo, collabora con l'azienda ed è in qualche modo coinvolto con il trattamento di dati e informazioni che rientrano nel campo di applicazione. Il personale è infatti responsabile, ciascuno per quanto di propria competenza, della segnalazione di tutte le anomalie e violazioni di cui dovesse venire a conoscenza;
- tutti i soggetti esterni che intrattengono rapporti e collaborano con l'azienda e che devono garantire il rispetto dei requisiti contenuti nella politica della privacy (*policy*);
- il titolare del trattamento quale responsabile deve:
  - condurre l'analisi dei rischi con le opportune metodologie e adottare le misure per la gestione del rischio;
  - stabilire le norme di comportamento necessarie alla conduzione sicura delle attività aziendali;
  - verificare le violazioni alla sicurezza, adottare le contromisure necessarie e controllare l'esposizione dell'azienda alle principali minacce e rischi;
  - organizzare la formazione e promuovere la consapevolezza del personale per tutto ciò che concerne la qualità, la sicurezza e la sicurezza delle informazioni;
  - verificare periodicamente l'efficacia e l'efficienza.

Il personale dell'azienda che, in modo intenzionale o riconducibile a negligenza, disattenda le regole di sicurezza stabilite e in tal modo provochi un danno, potrà essere perseguito nelle opportune sedi, nel pieno rispetto dei vincoli di legge e contrattuali.

8. MONITORAGGIO DEL SISTEMA GESTIONE PRIVACY

La direzione pianifica e verifica ciclicamente o almeno una volta all'anno l'efficacia e l'efficienza della gestione, in modo di assicurare un supporto adeguato all'introduzione di tutte le migliorie necessarie e di favorire l'attivazione di un processo di aggiornamento continuo.

Il Titolare del trattamento, quale responsabile, ha il compito di condurre operativamente la revisione di questa politica assieme al delegato.

La revisione deve verificare lo stato delle azioni preventive e correttive e l'aderenza alla politica privacy delle procedure in atto così come di quelle previste e non ancora applicate.

Deve inoltre tenere conto di tutti i cambiamenti che possono influenzare l'approccio alla gestione della sicurezza delle informazioni, includendo i cambiamenti organizzativi, l'ambiente tecnico, la disponibilità di risorse, le condizioni legali, regolamentari o contrattuali e dei risultati dei precedenti riesami.

Il risultato dell'intero processo di revisione periodica include tutte le decisioni prese e le azioni adottate in merito al miglioramento della sicurezza e rendicontazione (account ability).

9. INFORMAZIONE E FORMAZIONE

Ai fini della corretta e puntuale applicazione della disciplina relativa ai principi, alla liceità del trattamento, al consenso, all'informativa e, più in generale, alla protezione dei dati personali, CSU Zorzetto sostiene e promuove, all'interno della propria struttura organizzativa, ogni strumento di sensibilizzazione che possa consolidare la consapevolezza del valore della riservatezza dei dati e migliorare la qualità del servizio.

A tale riguardo, riconosce che uno degli strumenti essenziali di sensibilizzazione sia rappresentato dall'attività formativa del personale. Per garantire la conoscenza capillare delle disposizioni normative vigenti, al momento dell'ingresso in servizio, è data ad ogni dipendente una specifica comunicazione, con apposita clausola inserita nel contratto di lavoro, contenente il richiamo ai principi ed alle norme di cui al presente modello organizzativo, oltre che alle vigenti disposizioni nazionali e comunitarie.

Organizza periodicamente, nell'ambito della formazione continua e obbligatoria del personale, specifici interventi di formazione e di aggiornamento in materia di protezione dei dati personali, finalizzati alla conoscenza delle norme, alla prevenzione di fenomeni di abuso e illegalità nell'attuazione della normativa, all'adozione di idonei modelli di comportamento e procedure di trattamento, alla conoscenza delle misure di sicurezza per il trattamento e la conservazione dei dati, dei rischi individuati e dei modi per prevenire danni agli interessati. La formazione in materia di prevenzione dei rischi di violazione dei dati personali viene integrata e coordinata con la formazione in materia di trasparenza e di accesso, con particolare riguardo ai rapporti tra protezione dei dati personali, trasparenza accesso ai documenti amministrativi e accesso civico, semplice e generalizzato, nei diversi ambiti in cui opera. L'obiettivo di garantire un corretto trattamento dei dati, conforme ai requisiti previsti dalla normativa viene raggiunto da CSU Zorzetto anche e soprattutto grazie alla particolare attenzione risposta nei confronti della formazione di tutto il personale incaricato.

A tale scopo il Modello Organizzativo Privacy è divulgato presso il personale già in servizio e, nel caso di nuove risorse umane inserite in organico, fin dal momento del loro ingresso nella compagine di CSU Zorzetto. Per gli stessi fini di conoscenza eventuali aggiornamenti sono diffusi con gli strumenti ritenuti di volta in volta più efficaci.

Allo scopo creare un ecosistema favorevole nell'ambiente di lavoro e formare con particolare cura i soggetti che per il ruolo ricoperto risultano inseriti nel sistema per cui CSU Zorzetto:

- **adotta un piano formativo** con l'obiettivo di alfabetizzazione iniziale in materia di protezione dei dati personali, destinato a tutto il personale della società;
- **prevede l'erogazione di moduli formativi specifici** all'interno dei corsi per il ruolo ricoperto, sia in quelli organizzati all'immissione in servizio che al momento del cambio di mansione qualora sia di livello superiore o per ambito applicativo diverso;
- **prevede un piano di formazione programmato** con cadenza annuale sulla formazione erogata in ambito privacy a tutti i dipendenti della società;
- **conserva la documentazione** distribuita e la modulistica attestante la partecipazione agli interventi formativi.

La formazione dei soggetti autorizzati al trattamento e, ove ritenuto necessario, delle altre figure chiave dell'organizzazione, riguarda in particolare:

- gli aspetti generali della disciplina di protezione dei dati personali;
- le minacce, le vulnerabilità, la probabilità di accadimento e di conseguenza i rischi che minacciano i dati trattati;
- le conseguenze derivanti dalla violazione dei dati personali (*Data Breach*);
- le procedure da seguire in caso di violazione dei dati personali;
- le misure di prevenzione per evitare o almeno ridurre la probabilità di accadimento delle violazioni e le misure di mitigazione del danno in caso si verifichino;
- gli aspetti specifici della disciplina di protezione dei dati personali nel settore di azione di CSU Zorzetto;
- l'addestramento specifico per aggiornare il personale sulle misure di sicurezza e protezione dei dati personali ritenute adeguate e adottate dal Titolare del trattamento.

La formazione deve essere:

- adeguata al proprio sistema di trattamento dei dati personali;
- efficace nella trasmissione delle informazioni in materia di protezione dei dati personali;
- efficiente nel fornire strumenti per l'esecuzione delle procedure previste;
- documentabile, in quanto la formazione è parte integrante della *policy* di CSU Zorzetto e l'articolazione e gli esiti di tale attività devono essere sempre disponibili.

10. IMPEGNO DEGLI ORGANI DI GOVERNO

La direzione di CSU Zorzetto sostiene attivamente le attività inerenti alla gestione della privacy, e protezione dei dati personali, tramite indirizzi precisi, impegno evidente, incarichi espliciti e riconoscimento delle responsabilità specifiche relative alla sicurezza delle informazioni.

L'impegno della direzione si attua tramite un'adeguata struttura i cui compiti sono:

- **garantire** che siano identificati tutti gli obiettivi relativi alla sicurezza delle informazioni e che questi siano coerenti con la realtà della struttura a cui si riferiscono;
- **stabilire** i ruoli e relative responsabilità per lo sviluppo e il mantenimento del sistema nella sua completezza;
- fornire risorse sufficienti alla pianificazione, implementazione, organizzazione, controllo, revisione, gestione e miglioramento continuo;
- controllare che la sicurezza del Trattamento sia integrata in tutti i processi aziendali e che le conseguenti procedure e controlli siano sviluppati efficacemente;
- sostenere, valutare e approvare tutte le iniziative volte al miglioramento della sicurezza delle informazioni;
- attivare programmi per la diffusione della consapevolezza e della cultura della sicurezza delle informazioni.

Il Consorzio SU Zorzetto riconosce la propria responsabilità che discende dalla normativa vigente e si impegna a proteggere i dati personali che gli utenti affidano ad essa da perdita, uso improprio o accesso non autorizzato. Per la protezione dei dati personali degli utenti, l'azienda si avvale di tecnologie e procedure aziendali di protezione secondo le migliori pratiche (*best practices*) di volta in volta disponibili.

11. ORGANIGRAMMA, SISTEMA DI NOMINE E RESPONSABILITA'

Al fine di garantire la tutela dei diritti delle persone fisiche relativamente al trattamento dei dati personali, CSU Zorzetto garantisce sempre la precisa individuazione dei soggetti che ricoprono ruoli attivi. Ciò avviene con l'allestimento e il mantenimento efficiente nel tempo di un sistema tracciabile delle nomine e delle relative mansioni. In questo modo risulta di immediata comprensione la conseguente ripartizione delle responsabilità di ogni soggetto, parametrate alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento, nonché ai rischi per i diritti e le libertà delle persone fisiche analizzati ogni volta ritenuto necessario.

Quanto descritto trova riscontro nell'organigramma GDPR / privacy che viene aggiornato a cadenza periodica ritenuta più opportuna in relazione al settore di attività e all'articolazione della propria organizzazione oppure in occasione di qualsiasi variazione intervenuta.

In accordo con la normativa di riferimento e con la policy che discende dal presente Modello Organizzativo Privacy, costituiscono figure imprescindibili quelle di seguito descritte.

11.1 Impegni del Titolare del Trattamento

Conformemente a quanto previsto dalla normativa CSU Zorzetto è Titolare del trattamento e in tale ruolo si impegna a:

- **adeguare** il proprio assetto organizzativo per rendere il governo della privacy allineato ai dettami normativi;

- **adottare** le modalità operative necessarie alla corretta gestione degli adempimenti ai fini della protezione dei dati personali trattati;
- **assumere** le decisioni in ordine alle finalità, alle modalità del trattamento dei dati e agli strumenti utilizzati, ivi compreso il profilo della sicurezza, sia per i trattamenti svolti all'interno che all'esterno della propria struttura;
- **individuare** e designare i Responsabili del trattamento dei dati, impartendo loro le relative direttive e, se necessario, istruzioni specifiche;
- **vigilare** sulla puntuale osservanza delle disposizioni e istruzioni impartite a tutti i soggetti che hanno un ruolo attivo nel trattamento dei dati personali;
- **garantire** sempre il pieno controllo sulla piramide organizzativa di cui è al vertice, concedendo autorizzazioni generali o specifiche ai responsabili del trattamento secondo criteri di opportunità nelle diverse situazioni ed esprimendo o negando il gradimento nei confronti di sub-responsabili eventualmente proposti dai responsabili assumendo così un ruolo di effettivo controllo e indirizzo.

Inoltre, si impegna a garantire l'esercizio dei diritti degli interessati e a tal scopo individua e mette in pratica apposite procedure al fine di informare gli interessati e garantire a ciascuno di essi almeno il:

- **diritto all'accesso**, cioè di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano e di averne accesso. In particolare, l'interessato ha diritto di conoscere l'origine dei dati personali; le finalità e modalità del trattamento; la logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici; gli estremi identificativi del titolare, dei responsabili e degli eventuali rappresentanti designati; l'elenco dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza a qualsiasi titolo in linea con la normativa e quello dei soggetti autorizzati al trattamento;
- **diritto alla rettifica**, cioè di ottenere l'aggiornamento, la correzione ovvero, quando vi ha interesse, l'integrazione dei dati;
- **diritto alla cancellazione**, cioè di ottenere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
- **diritto all'opposizione**, cioè di limitare od opporsi, per motivi legittimi, al trattamento, seguendo le modalità descritte dalle norme vigenti.

Al fine di esercitare i diritti sopra descritti, CSU Zorzetto si impegna a rispondere senza ritardo alle richieste presentate da parte dell'interessato direttamente ad esso, ai Responsabili o ai soggetti autorizzati appositamente nominati, nelle forme e modalità nonché attraverso i mezzi ritenuti più idonei.

11.2 Responsabile del Trattamento

Il Responsabile del trattamento dei dati è il soggetto, persona fisica o giuridica, nominato dal Titolare al fine di garantire nelle operazioni di trattamento l'attuazione delle misure di sicurezza previste dalla normativa e dal presente Modello Organizzativo Privacy.

Il soggetto preposto allo svolgimento della funzione viene individuato tra quelli in possesso dei necessari requisiti e con adeguate garanzie. Tra le sue funzioni sono comprese quelle di:

- **osservare** le procedure in materia di protezione dei dati personali adottate dal Titolare;
- **organizzare**, gestire e supervisionare tutte le operazioni di trattamento dei dati personali

affinché esse vengano effettuate nel rispetto delle disposizioni di legge e predisporre tutti i documenti nonché le misure tecniche organizzative richiesti dal Codice e dal Regolamento;

- **adottare** e verificare il rispetto delle misure di sicurezza indicate dal Codice e dal Regolamento e la conformità nel tempo dei sistemi e delle misure di sicurezza;
- **redigere** e aggiornare il registro delle attività di trattamento, qualora sia necessario;
- **informare** il Titolare del trattamento di tutte le misure adottate e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal Titolare del trattamento o da un altro soggetto da questi incaricato al compito specifico;
- **nominare** i soggetti autorizzati che svolgono tali funzioni per suo conto, conservando i relativi estremi identificativi, definendo gli ambiti di operatività consentiti e verificando almeno annualmente il relativo operato per controllarne la rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti il trattamento dei dati personali;
- **nominare** i soggetti autorizzati al trattamento dei dati nelle altre funzioni ritenute necessarie conferendo loro apposite istruzioni sulle norme e le procedure da osservare e provvedendo alla relativa formazione;
- **controllare** le operazioni di trattamento svolte dai soggetti autorizzati sottoposti alla propria responsabilità e la conformità all'ambito di trattamento consentito;
- **redigere** e aggiornare la lista dei nominativi dei soggetti autorizzati sottoposti alla propria responsabilità e verificarne almeno annualmente l'ambito di trattamento consentito;
- **proporre** al Titolare del trattamento dei dati la nomina di soggetti per il ruolo di sub-Responsabile del trattamento dei dati in relazione all'affidamento agli stessi di determinate attività;
- **attuare** gli obblighi di informazione ed acquisizione del consenso, quando richiesto, nei confronti degli interessati;
- **garantire** all'interessato che ne faccia richiesta l'effettivo esercizio dei diritti previsti dalla normativa di settore inoltrando al Titolare del trattamento le richieste pervenute nel caso non possano essere evase autonomamente;
- **distruggere** i dati personali alla fine del trattamento nei casi previsti dal Regolamento, secondo le procedure atte a garantire la sicurezza degli stessi e provvedere alle formalità di legge e agli adempimenti necessari;
- **comunicare** immediatamente al titolare non oltre le 24 ore successive al loro ricevimento, ogni richiesta, ordine o attività di controllo da parte del Garante o dell'Autorità Giudiziaria;
- **osservare** le procedure in materia di protezione dei dati personali adottate dal Titolare del trattamento;

Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il Titolare del trattamento può modificare la propria struttura per conseguire i migliori risultati di protezione variando opportunamente l'articolazione del proprio sistema di gestione.

11.3 Soggetti autorizzati al trattamento

Il Titolare del trattamento (o il Responsabile del Trattamento) nomina, presso le Unità Organizzative in cui vengono svolti i trattamenti, i soggetti autorizzati al trattamento dei dati (o soggetto *designato*).

Il soggetto autorizzato effettua tutte le operazioni di trattamento dei dati personali attinenti all'attività lavorativa di competenza dell'area di appartenenza e opera sotto l'autorità del Titolare (o del Responsabile del Trattamento), attenendosi alle istruzioni dallo stesso impartite

nonché alle specifiche procedure che regolamentano le modalità di utilizzo delle banche dati cui lo stesso abbia accesso.

In particolare, i compiti a esso attribuiti sono così sintetizzati:

- **segnalare** al Titolare del trattamento, eventuali richieste ricevute da parte dell'interessato sull'esercizio dei relativi diritti, nonché attenersi alla procedura interna sull'esercizio dei diritti;
- **avvisare** il Titolare del trattamento qualora, nello svolgimento di un'attività, dovesse riscontrare il trattamento di nuovi dati e finalità per cui risultasse necessario aggiornare il registro dei trattamenti ed eseguire almeno un'analisi dei rischi, in applicazione dei principi di *privacy by design* e *privacy by default*;
- **informare** immediatamente il Titolare del trattamento qualora le istruzioni ricevute risultino non conformi alla normativa sulla protezione dai dati;
- segnalare al Titolare del trattamento eventuali accessi non autorizzati;
- **rilasciare** all'interessato l'informativa e acquisire il consenso laddove necessario, secondo le istruzioni impartite dal Titolare del trattamento (o del Responsabile del trattamento di riferimento).

11.4 Amministratore di Sistema

La figura professionale che, in ambito informatico, mantiene, configura e gestisce un sistema di elaborazione dati o sue componenti, ivi inclusi sistemi software complessi (*system administrator*), ovvero una base dati (*database administrator*), ovvero reti e apparati di telecomunicazione di sicurezza (*network administrator*) è nominata persona autorizzata al trattamento dei dati personali con la qualifica specialistica di Amministratore di Sistema.

L'attribuzione delle funzioni di Amministratore di Sistema avviene previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale fornisce idonea garanzia del pieno rispetto delle vigenti disposizioni in materia, ivi compreso il profilo relativo alla sicurezza.

La nomina ad Amministratore di Sistema deve essere individuale, esplicitata in forma scritta, con l'indicazione analitica degli ambiti di applicazione di operatività consentiti in base al profilo di autorizzazione assegnato.

In generale, l'Amministratore di sistema ha le seguenti responsabilità:

- **sovraintendere** alle risorse dei sistemi computerizzati al fine di consentirne una corretta ed efficiente utilizzazione;
- **fornire** guida e supporto ai soggetti autorizzati in merito al trattamento dei dati personali in accordo con il Titolare del trattamento;
- **amministrare** e gestire la sicurezza informatica operando anche come gestore e custode delle password;
- **effettuare** periodici controlli e verifiche tecniche, nell'ambito delle responsabilità assegnate, in merito a quanto previsto dal Regolamento Informatico;
- **individuare** i soggetti a cui affidare l'incarico di manutentore del sistema stesso.

L'amministratore di Sistema che provvede alla designazione dei soggetti incaricati alla manutenzione deve preventivamente informare il Titolare del Trattamento e deve formalizzare per iscritto l'attribuzione dell'incarico eventualmente specificando i limiti dell'intervento e le manutenzioni richieste. Per manutenzione s'intende non soltanto l'intervento tecnico diretto ad eliminare eventuali avarie hardware, ma anche gli interventi volti alla ricostruzione di archivi

che dovessero in qualche modo risultare danneggiati o corrotti oltre all'intervento tecnico diretto ad eliminare eventuali avarie al software di sistema e all'applicativo utilizzato.

Per consentire all'Amministratore di Sistema di svolgere adeguatamente le proprie funzioni, allo stesso vengono concesse dal Titolare del trattamento le "Autorità di sistema", che consistono nell'assegnazione di attributi, privilegi, o accessi che consentono la gestione delle "risorse critiche del sistema operativo", ovvero degli oggetti informatici necessari al funzionamento dei sistemi e del servizio di elaborazione dati.

L'elenco dei soggetti nominati Amministratori di Sistema è conservato adeguatamente.

12. MISURE DI SICUREZZA GENERALI

12.1 La gestione della sicurezza: ruoli e responsabilità

La responsabilità delle attività di impostazione e coordinamento dei sistemi che garantiscono la sicurezza e la tutela di tutti i dati oggetto di trattamento sono in carico ai relativi ruoli inseriti nell'organico di CSU Zorzetto. Tali sistemi possono essere sia logici che fisici e la responsabilità comprende la loro gestione diretta o tramite fornitori esterni.

In considerazione della complessità delle implicazioni relative alla sicurezza logica, è redatto il Regolamento Informatico.

12.2 Misure per garantire la protezione dei dati

Sono le misure di sicurezza volte a minimizzare i rischi che le informazioni siano rivelate o modificate senza autorizzazione, ovvero perse o alterate accidentalmente o intenzionalmente.

Queste comprendono un sistema di autenticazione per assicurare che la persona che accede al sistema nelle sue diverse articolazioni sia identificata con certezza, basato su codice identificativo e password individuale segreta, nonché un sistema di autorizzazione che prevede che a ciascuna persona che accede al sistema sia assegnato un profilo di accesso che definisce i dati ai quali l'utente è autorizzato ad accedere e, ove applicabile, le operazioni che per ciascun dato o gruppo di dati è autorizzato ad eseguire (consultazione, inserimento, modifica, cancellazione).

Ad eccezione degli Amministratori di Sistema definiti e nominati secondo le disposizioni del Modello Organizzativo Privacy, nessun dipendente di CSU Zorzetto è Amministratore di Sistema della propria macchina e tutti gli utenti che dispongono di una postazione informatica sono censiti.

Per ridurre i rischi di indisponibilità (parziale o totale) nell'accesso al sistema informatico di CSU Zorzetto sono previste una serie di attività, in particolare al momento dell'assunzione o della dimissione delle risorse umane con la procedura di allestimento o dismissione dell'utenza personale. Sempre al fine di controllo si procede a verificare con cadenza semestrale che la lista dei dipendenti cessati sia coerente con le utenze disabilitate.

Tutti i dispositivi di CSU Zorzetto concessi in dotazione ai dipendenti vengono formattati a seguito delle dimissioni degli stessi al fine di rimuovere tutti i dati personali contenuti al loro interno.

Tutti i dipendenti di CSU Zorzetto sono pertanto tenuti ad assicurarsi che venga correttamente eseguito il passaggio di consegne affinché venga assicurata la continuità dei servizi erogati

e la conservazione dei documenti di lavoro.

12.3 Scrivania sgombra e schermo inattivo (*clean desk & clear screen Policy*)

La politica della ***scrivania sgombra*** (*Clean Desk Policy*) e dello **schermo inattivo** (*Clear Screen Policy*) è una delle migliori strategie da attuare per ridurre il rischio di violazioni della sicurezza della postazione di lavoro.

Lo scopo di tale politica è stabilire requisiti minimi per prevenire violazioni accidentali o dolose dei dati personali (*Data Breach*) e responsabilizzare i soggetti che nelle attività lavorative si trovano a loro contatto.

Di seguito sono elencati i comportamenti virtuosi da applicare:

- i dipendenti sono tenuti a garantire che tutte le informazioni sensibili o confidenziali in formato elettronico o cartaceo siano messe al sicuro nella propria postazione di lavoro, in particolare alla fine della giornata lavorativa e in caso di assenza prolungata;
- i computer devono essere bloccati quando le postazioni di lavoro non sono occupate;
- tutti i computer devono essere spenti alla fine della giornata lavorativa;
- qualsiasi informazione e/o dato particolare/sensibile deve essere rimosso dalla scrivania e chiuso a chiave in un cassetto quando la postazione di lavoro non è occupata e alla fine della giornata lavorativa;
- le cartelle contenenti informazioni riservate e/o sensibili e/o categorie particolari di dati personali devono essere tenute chiuse e bloccate quando non utilizzate;
- le chiavi utilizzate per accedere alle informazioni riservate e/o ai dati sensibili e/o alle categorie particolari di dati personali non devono essere lasciate su una scrivania non presidiata;
- i laptotp devono essere conservati in un cassetto se non utilizzati;
- le password non possono essere lasciate su note adesive attaccate sopra, sotto o nei pressi di un computer, né possono essere lasciate per iscritto in posizione accessibile;
- le stampe contenenti informazioni riservate e/o dati particolari/sensibili devono essere immediatamente rimosse dalle stampanti;
- al momento dello smaltimento, i documenti riservati o contenenti informazioni riservate e/o sensibili e/o categorie particolari di dati personali devono essere distrutti e, ove presenti, triturati nei distruggidocumenti appositi;
- le lavagne contenenti informazioni riservate e/o sensibili e/o categorie particolari di dati personali devono essere cancellate;
- i dispositivi portatili come laptop, smartphone o tablet non devono mai essere lasciati sbloccati e incustoditi;
- tutti i dispositivi di archiviazione di massa come CDROM, DVD o chiavi USB contenenti informazioni riservate e/o sensibili e/o categorie particolari di dati personali devono essere conservati in cassetti chiusi a chiave.

Il dipendente che viola queste norme di comportamento è soggetto alle azioni disciplinari previste, fino al licenziamento.

12.4 Livelli di sicurezza

L'amministrazione della sicurezza logica segue i seguenti criteri generali:

- applicazione del principio del minimo privilegio, secondo cui la definizione dei profili standard da assegnare agli utenti, con le autorizzazioni necessarie all'espletamento delle rispettive

mansioni (definite per ruoli e competenze), avviene alla luce delle effettive esigenze operative. A tal scopo viene limitato l'accesso logico a reti, sistemi e basi dati;

- validazione delle richieste di accesso alla rete è verificata automaticamente dal sistema stesso prima di consentire l'accesso ai dati, tramite un sistema di autenticazione costituito da username e password;
- sono adottate delle indicazioni per la gestione delle password che indicano la lunghezza, la complessità, la durata, la conservazione sicura richiesta nel caso di trattamenti dei dati effettuati con strumenti elettronici;
- sono previsti sistemi per la periodica validazione e il censimento delle utenze e delle abilitazioni;
- sono adottate tecniche e metodologie per la verifica continua dell'utilizzo dei sistemi applicativi e per il controllo del traffico di rete generato, al fine di garantire un pronto intervento in caso di attività anomale;
- sono previsti presidi rafforzati per l'accesso da remoto, in particolare nei confronti di utenti appartenenti a soggetti terzi;
- è prevista la revisione periodica delle misure di sicurezza, al fine di prevenire violazioni dei dati personali (*Data Breach*);
- sono organizzate sessioni di formazione dei dipendenti, nonché regolamenti e altre forme di documentazione interna, al fine di rendere gli stessi edotti dei rischi in materia di sicurezza delle informazioni e di protezione dei dati personali;
- sono previsti periodici controlli al fine di verificare l'adeguatezza, l'affidabilità complessiva e la tutela del sistema informativo.

Particolari oneri e obblighi

Il Sig. Maurizio Foffano, conformemente a quanto previsto dall'articolo 12 della Legge del 31 dicembre 2012 n. 247, dichiara di possedere idonea Polizza assicurativa della responsabilità civile professionale a garanzia degli eventuali danni provocati da errori materiali ed inadempienze commessi nello svolgimento della propria attività professionale.

La polizza sarà mantenuta in essere con le caratteristiche minime indicate (salva la facoltà di variazione della Compagnia assicuratrice e di eventualmente aumentare il massimale garantito) per tutta la durata della nomina.

Il mancato rinnovo da parte del Responsabile della Sicurezza dei dati della suddetta polizza è considerato grave inadempimento che costituisce clausola risolutiva espressa ai sensi dell'art. 1456 del Codice Civile.

14. SOSPENSIONE DEL SERVIZIO

L'Azienda non può sospendere con decisione unilaterale i servizi oggetto del contratto nemmeno nel caso in cui siano in atto controversie con il TITOLARE.

La sospensione per decisione unilaterale dell'Azienda costituisce inadempienza contrattuale e comporta la risoluzione del contratto, fatta comunque salva la facoltà di procedere nei confronti dell'Azienda per tutti gli oneri conseguenti e derivanti dalla risoluzione contrattuale e per l'eventuale risarcimento del danno.

15. DISPOSIZIONI FINALI

Ferma la possibilità di attivare procedure di composizione stragiudiziale delle vertenze, tutte le controversie relative all'interpretazione del presente contratto e all'esatta esecuzione delle prestazioni dovute, saranno devolute al Foro di Venezia.
Il presente atto è frutto di ampia e paritaria concertazione tra le parti, e non contiene clausole vessatorie,
Per quanto non espressamente previsto, trova applicazione ogni disciplina normativa, legislativa, comunitaria e nazionale, e regolamentare sui temi oggetto del presente atto.

Premesso ciò si impegna all'aggiornamento ciclico.

C.S.U. G. Zorzetto Soc. Coop. Sociale
Via Asseggiano, 41/N 30174 Venezia Mestre
Tel 041 928922 Fax 041 914226
info@csuzorzetto.it www.csuzorzetto.it
www.csuzorzetto.it - R.I./C.F./P.IVA 02894130273
Albo Coop. A125873 - CCIAA Ve R.E.A. 246451

TITOLARE DEL TRATTAMENTO

DATA

DELEGATO