NOMINA A RESPONSABILE DEL TRATTAMENTO AI SENSI DELL'ART. 28 DEL REGOLAMENTO UE 2016/679

Spett.le Gobesso Sandro – Agenzia GS
Via del Forno n. 3 - 19125 – La Spezia
Partita Iva 01461480111
Codice Fisc. GBSSDR67R03E463E

Fondazione " Manlio Canepa" Onlus P.IVA: 01341730115 in persona del legale rappresentante pro tempore, ai sensi dell'art. 28 del REGOLAMENTO UE 2016/679, in qualità di Titolare del Trattamento, Vi comunica la nomina a responsabile del trattamento dei dati personali nell'ambito dell'incarico a Voi conferito e per le aree di competenza di seguito definite:

Area "trattamento dati" inerenti la gestione dei dati relativi ai nostri dipendenti, collaboratori interni ed esterni per la consulenza sugli adempimenti formali relativi al Regolamento UE 2016/679.		
Consulenza e adempimenti formali sul Regolamento UE 2016/679.	Dati comuni	• Dati anagrafici relativi alle risorse interne ed esterne • Dotazioni e ubicazione delle risorse interne

A tal fine vengono fornite istruzioni per l'assolvimento del compito assegnato:

a) trattare i dati del Titolare in modo lecito, secondo correttezza ed avendo cura che l'accesso ad essi sia possibile solo a soggetti autorizzati al trattamento e impegnandosi a trattare i dati personali esclusivamente per gli scopi che sono oggetto dell'incarico conferito;

b) nominare per iscritto come incaricati/autorizzati del trattamento dei dati personali i propri dipendenti o eventuali altre persone fisiche che siano deputati a trattare i dati messi a disposizione dal Titolare medesimo, fornendo loro precise istruzioni operative, anche sotto il profilo delle misure minime di sicurezza, conformemente alle prescrizioni del Regolamento UE 2016/679

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, mettere in atto misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, conformemente a quanto disposto dall'art. 32 Regolamento UE 2016/679.

d) Fornire al Titolare le informazioni relative ad eventuali soggetti a cui intende affidare le attività o parte di esse (subappaltatori, subfornitori, ecc.) ove previsto contrattualmente ;

e) gestire il sistema informatico nel quale sono conservati i dati personali secondo le indicazioni contenute nel presente incarico ed in osservanza a quanto previsto dal Regolamento UE 2016/679 e attenendosi ad ogni eventuale ed ulteriore disposizione da parte del Titolare;

f) assegnare e gestire un sistema di autenticazione informatica nell'accesso agli strumenti ed alle applicazioni informatiche utilizzate, mediante l'uso di parole chiave e/o codici identificativi personali da assegnare agli incaricati/autorizzati al trattamento dati, con custodia delle relative credenziali, e loro disattivazione nei casi previsti dalla legge;

g) adottare programmi antivirus, firewall e/o altri strumenti software od hardware di uso comune atti a garantire la sicurezza dei dati, verificandone l'installazione, l'aggiornamento ed il funzionamento;

h) provvedere al ricovero periodico dei dati con copie di backup, vigilando sulle procedure all'uopo attivate, ed assicurando la qualità delle copie di backup e la loro conservazione in luogo adatto e sicuro;

i) Assistere il titolare del trattamento, nella misura in cui ciò è possibile, nell'adempimento dell'obbligo relativo alla risposta alle richieste degli interessati circa l'esercizio dei suoi diritti quali l'accesso, rettifica, cancellazione, opposizione, limitazione trattamento, portabilità dei dati e al diritto di non essere oggetto di una decisione individuale automatizzata quale la profilazione.

l) comunicare prontamente al titolare del trattamento qualsiasi situazione di cui venga a conoscenza nell'erogazione del servizio, che possa compromettere il corretto trattamento dei dati personali impegnandosi, in particolare all'osservanza dell'art. 33, comma 2 (Notifica di una violazione dei dati personali all'autorità di controllo) del citato Regolamento UE 2016/679, e quindi ad informare tempestivamente il Titolare senza ingiustificato ritardo della violazione di cui sia venuto a conoscenza;

m) assicurare che i dati personali siano conservati per il tempo strettamente necessario all'esecuzione delle attività /servizi richiesti dal Titolare e comunque non oltre i termini di legge o quelli di volta in volta indicati dal Titolare medesimo, utilizzando i dati solo per le finalità connesse allo svolgimento dell'attività inerente il Servizio offerto, con divieto di qualsiasi altra diversa utilizzazione

n) all'atto della conclusione del servizio, cancellare in modo permanente dai propri sistemi elettronici e/o archivi cartacei i dati comunicati dal Titolare, entro i normali tempi tecnici a ciò necessari.

Il Titolare del Trattamento

(Fondazione " Manlio Canepa" Onlus)

Il Responsabile del trattamento

(Gobesso Sandro)

Luogo e data,_____

REGISTRO DEL RESPONSABILE DEL TRATTAMENTO
Regolamento UE 2016/679 art. 30

TITOLARE DEL TRATTAMENTO	
Denominazione	Fondazione " Manlio Canepa" Onlus
Partita Iva	01341730115
Codice Fiscale	
Indirizzo sede legale	Viale della Vittoria, 39 19032 –Lerici (SP)
Legale rappresentante	Roberto De Simone

DATI DI CONTATTO	
fondazionemanliocanepa@gmail.com	0187/971997

RESPONSABILE DEL TRATTAMENTO	
Denominazione	Gobesso Sandro – Agenzia GS
Partita Iva	01461480111
Codice Fiscale	GBSSDR67R03E463D
Indirizzo sede legale	Via Del Forno n. 3 – 19125 La Spezia

DATI DI CONTATTO	
privacy@agenziags.it	0187/284510

DESCRIZIONE TIPOLOGIA DI TRATTAMENTO EFFETTUATO PER CONTO DEL TITOLARE DEL TRATTAMENTO
Area "trattamento dati" inerenti la gestione dei dati delle risorse interne ed esterne da voi forniti per la predisposizione della documentazione relativa all'incarico ricevuto

FINALITA' DEL TRATTAMENTO
Svolgimento delle attività connesse all'incarico ricevuto inserente la predisposizione della documentazione richiesta

CATEGORIA INTERESSATI
Dati anagrafici delle vostre risorse interne ed esterne e le varie autorizzazione e dotazioni a loro concesse sulla gestione dei dati personali

CATEGORIE DI DATI PERSONALI
Dati Anagrafici delle risorse interne (nome, cognome, codice fiscale) – informazioni su autorizzazioni concesse alle risorse interne tra le quali l'uso di apparecchi informatici o mobili – Dati anagrafici e di contatto delle risorse esterne che utilizzato dati per conto del titolare.

CATEGORIE DI DESTINATARI A CUI I DATI POTRANNO ESSERE COMUNICATI
- Dipendenti / Collaboratori autorizzati al trattamento dei dati personali ai sensi e per gli effetti degli artt. 5,24, 29 e 32 del Regolamento UE 2016/679. - Soggetti esterni possono venire a conoscenza dei dati per finalità relative ad assistenza informatica, erogazione di servizi di consulenza previsti dal mandato, consulenti e liberi professionisti anche in forma associata con finalità collaborazione con cui il Titolare abbia stipulato accordi.

TRASFERIMENTO DATI ALL'ESTERO
Non è previsto, da parte del Responsabile, il trasferimento dei dati all'estero.

TERMINI PER LA CANCELLAZIONE DEI DATI
I dati vengono conservati per tutto il tempo relativo allo svolgimento dell'incarico contrattualizzato con il titolare oltre che per gli annessi adempimenti e conservazione dello storico.

DESCRIZIONE GENERALE DEEL MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE

- *I parametri di autenticazione al sistema o al programma sono attribuiti ad personam.(**V. Dettaglio Password Policy e Gestione Account)***

- *Nel caso in cui sul disco locale del computer fossero trattati dati personali non presenti anche sul disco di rete, tali dati verranno salvati almeno settimanalmente.*

- *Nel caso in cui l'aggiornamento automatico dell'Antivirus non fosse impostato o non funzionasse correttamente l'incaricato è consapevole di dover avvisare il Titolare il quale direttamente o tramite l'intervento di tecnici informatici dovrà risolvere il problema nel tempo più breve.*

- *Nel caso in cui l'Incaricato si dovesse allontanare dal computer dovrà prima mettere in sicurezza il computer in modo che altre persone non possano trattare dati personali con le sue credenziali di autorizzazione disconnettendo l'utente oppure impostando l'opzione "al ripristino proteggi con password" nel salvaschermo.*

- *Sono state pianificate dal Titolare procedure in caso di sostituzione di strumenti informatici : il Pc dismesso se rimane presso gli uffici dovrà essere reso inutilizzabile; se ceduto a terzi dovrà essere richiesta ampia garanzia, da parte del tecnico incaricato allo smobilizzo, che il disco venga formattato (bassa formattazione – doppio zero o doppio spazio) o reso inutilizzabile. **(V. Dettaglio Politica per la cancellazione sicura e lo smaltimento dei supporti elettronici).** La medesima misura sarà attivata su qualsiasi disco o altro strumento che contiene dati.*

Password Policy e Gestione degli Account

- *I dipendenti/Collaboratori accedono alle risorse informatiche solo ed esclusivamente previa presentazione delle proprie credenziali di identificazione e autenticazione.*

- *Le credenziali di identificazione ed autenticazione sono composte da un identificativo univoco dell'utenza (user-id) e da una password, quest'ultima strettamente personale, non comunicabile e non condivisibile con terze persone.*

- *La password dovrà essere composta da almeno 8 caratteri e non dovrà essere riconducibile all'incaricato e dovrà essere composta da una combinazione di lettere maiuscole-minuscole, numeri, e altri caratteri speciali.*

- *la password è conosciuta soltanto dall'incaricato che autonomamente dovrà cambiarla ogni 3 mesi (L'incaricato potrà cambiarla anche più spesso e comunque ogni qualvolta dovesse ravvisare il rischio di compromissione della segretezza della password.)*

- *l'utente è stato reso consapevole di non condividere le proprie password con nessun altro utente, inclusi colleghi*

- *l'utente dovrà cambiare al primo accesso la prima password ricevuta a seguito della creazione di un nuovo account aziendale.*

Utilizzo delle Risorse di Rete

- *Il personale autorizzato deve utilizzare le risorse di rete a disposizione (ad es. posta elettronica, internet) in maniera responsabile e al solo scopo di espletare le proprie attività lavorative, evitando comportamenti e modalità di utilizzo che possono causare oltre che una perdita di produttività, anche rischi per l'integrità, la riservatezza e la*

disponibilità delle informazioni aziendali.

Accesso ed utilizzo della rete Internet

Il Titolare fornisce al personale autorizzato l'accesso alla rete Internet, al fine di facilitare la conduzione delle proprie attività lavorative. L'uso occasionale della rete Internet per motivi personali non deve interferire con le attività lavorative:

Pertanto, l'uso della rete Internet è consentito per scopi leciti e professionali, e deve essere fatto in maniera responsabile. In particolare,

- *Il download di programmi, modelli di documenti o altri files non necessari per il normale svolgimento del lavoro non è consentito in quanto aumenta il rischio di intrusione ed il pericolo alla riservatezza e integrità dei dati.*
- *Non è consentito l'utilizzo di sistemi peer-to-peer P2P di condivisione di files e/o cartelle per i soliti motivi sopra esposti.*
- *È consentito l'accesso a siti che consentano la visione delle proprie email (webmail) ma non è consentito il download di allegati.*

Accesso ed utilizzo della Posta elettronica

L'accesso alla posta elettronica aziendale (e-mail) viene fornito al personale autorizzato al fine di svolgere le attività lavorative o in adempimento di contratti di collaborazione con persone esterne all'azienda. Gli operatori sono stati resi edotti delle minacce a cui è potenzialmente esposto questo mezzo, evitando ad esempio l'apertura di allegati ai messaggi di posta (anche se provenienti da persone conosciute) il cui nome del file termini in (abbia estensione) .COM .EXE .VBS .SCR .PIF, o che abbia un'estensione ambigua o sconosciuta (gli allegati possono, infatti, contenere virus o codici nascosti di natura dolosa che possono comportare la divulgazione di password o la compromissione di dati aziendali).

Gli operatori sono consapevoli che in caso di invio di una mail a più destinatari (che non abbiano acconsentito a comunicare agli altri il proprio indirizzo) è necessario nascondere i nomi e gli indirizzi dei destinatari nei messaggi di posta elettronica usando l'opzione Ccn, che significa "copia per conoscenza nascosta". Il campo Ccn consente di inviare le comunicazioni ai destinatari appropriati, rispettando al contempo la loro privacy non rivelandone l'identità.

Modalità di Backup dei dati su supporto elettronico.

- Al fine di garantire l'integrità e la pronta disponibilità dei dati in caso di distruzione o danneggiamento **il Titolare si è dotato di strumenti e procedure di backup** che avvengono in automatico con frequenza quotidiana su :
- **Nas synology con doppio disco**

Per quanto riguarda il rischio di distruzione o copia da parte di persone non autorizzate al trattamento dei dati elettronici, le misure tecniche, procedurali ed organizzative sono le seguenti: Sono stati presi in considerazione anche i seguenti rischi :

- ***distruzione dei dati;***
- ***accesso non autorizzato ai dati;***
- ***perdita dei dati;***

Per evitare il rischio distruzione, è stato installato un antivirus professionale che viene aggiornato automaticamente tramite collegamento internet.

Per evitare il rischio accesso non autorizzato dall'esterno è stato installato un firewall professionale per la gestione della protezione perimetrale.
Periodicamente vengono controllati i files di log del firewall in modo da valutare eventuali tentativi di intrusione.

Per evitare il rischio di perdita di dati è stata pianificata la copia del database e degli archivi contenenti la posta elettronica secondo le modalità sopra descritte.
Tutti i salvataggi vengono criptati con una chiave di sicurezza personale prima del trasferimento.

Protezione degli archivi cartacei

Per quanto riguarda il rischio di accesso da parte di persone non autorizzate ai dati cartacei, le misure tecniche, procedurale ed organizzative adottate sono le seguenti:

- *I dati particolari sono custoditi in armadi e cassetti chiusi a chiave e tutti gli archivi si trovano in locali dotati di serratura. Durante l'orario di lavoro i locali sono costantemente controllati dalle persone che vi lavorano. Dopo l'orario di chiusura possono accedere all'archivio solo le persone preventivamente autorizzate.*

- *Durante gli orari di ricevimento il Titolare e gli altri soggetti autorizzati al trattamento avranno cura di non lasciare incustoditi sulla scrivania fascicoli/ pratiche e/o appunti contenenti dati personali*

- *Nel caso di trattamento di dati particolari, se l'incaricato dovesse interrompere il trattamento dovrà riporre tali dati nel luogo dove sono custoditi o, in alternativa, custodirli personalmente nel caso in cui si dovesse spostarsi in altra stanza dell'ufficio.*

- *Il titolare / autorizzati al trattamento distruggeranno personalmente le copie di stampa che, per il particolare contenuto di riservatezza o per la sensibilità dei dati, non si prestano al riuso per bozze.*

- *Il Titolare/ autorizzati al trattamento presteranno attenzione a non lasciare posta e comunicazioni trasmesse a mezzo fax/posta incustodite e visibili a terzi.*

Le misure di sicurezza adottate si applicano sia ai documenti originali che alle loro copie.

Il Responsabile del trattamento

(Gobesso Sandro)

Il Titolare del trattamento
(per presa visione)

(Fondazione " Manlio Canepa" Onlus)