Istruzioni funzionali al trattamento di dati personali rivolte al personale che agisce sotto l'autorità del Titolare del trattamento, ai sensi e per gli effetti dell'art. 29 Regolamento (UE) 2016/679 (GDPR)

Gent.ma/Egr. Dott.ssa/Dott._____

Premesso che:
Il Regolamento (UE) 2016/679 (GDPR), disciplina i principi e le norme a tutela delle persone fisiche con riguardo al trattamento dei dati personali. Specificamente, il GDPR prevede che all'interno di ogni realtà aziendale sia costituita una gerarchia funzionale alla sua applicazione, comprendente le figure del titolare, del responsabile e di "*chiunque agisca sotto l'autorità del Titolare o del responsabile, che abbia accesso a dati personali*". Tale gerarchia non comporta alcuna modifica della qualifica professionale o delle mansioni assegnate ai dipendenti. In particolare l'Art. 29 GDPR prevede che chiunque agisca sotto l'autorità del titolare del trattamento, che abbia accesso a dati personali, non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento. Nell'ambito dello svolgimento delle Sue funzioni, Lei viene necessariamente a conoscenza dei dati personali contenuti nelle banche dati aziendali (cartacee e informatiche) e può avere accesso ai dati ed effettuare attività di trattamento sugli stessi.
Pertanto con la presente **Fondazione Exodus Onlus**, Titolare del trattamento ai sensi dell'articolo 24 del Regolamento (UE) 2016/679 (GDPR), in persona del legale rappresentante pro-tempore, La

Nomina

Autorizzato al trattamento dei dati personali e Le fornisce le istruzioni operative che dovrà rispettare nell'esecuzione delle Sue mansioni lavorative che comportino il trattamento di dati **personali** (qualsiasi informazione riguardante un interessato, 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 – cfr. art. 4, c. 1, n. 1), ed eventualmente -qualora la mansione lo preveda- di **categorie di dati particolari** (ad es. origine razziale ed etnica, opinioni politiche, convinzioni religiose o filosofiche, iscrizione sindacale, dati biometrici o relativi alla salute – cfr. art. 9 GDPR) e dati **relativi a condanne penali e reati** (cfr. art. 10 GDPR).
Per **trattamento** di dati deve intendersi: *"qualunque operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme 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"*.
Per **interessato** deve intendersi: "*persona fisica indentificata o identificabile*".

Principi del Trattamento:
Ai sensi dell'art. 5 GDPR Le ricordiamo che i dati personali devono essere:
a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («principio di liceità, correttezza e trasparenza»);
b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; («principio di limitazione della finalità»);
c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («principio di minimizzazione dei dati»);
d) 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 («principio di esattezza»);
e) 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; («principio di limitazione della conservazione»);
f) 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 («principio di integrità e riservatezza»).

Accesso a banche dati aziendali
Le banche dati cui potrà accedere per effettuare i trattamenti, strettamente pertinenti alle mansioni svolte e per le finalità previste dal titolare del trattamento, rispettando i principi fondamentali sanciti dall'art. 5 GDPR, sono le seguenti:

- Anagrafiche utenti e dei famigliari degli utenti;
- Categorie particolari di dati personali relativi agli utenti della struttura, quali dati relativi alla salute, tra cui: esiti di visite/controlli medici, percorsi riabilitativi e terapeutici, certificati sullo stato di salute dell'utente;
- Dati relativi a condanne penale e reati degli utenti della struttura per la gestione dei rapporti con le autorità pubbliche competenti.

I programmi, i sistemi e gli strumenti cui potrà accedere per effettuare i trattamenti, strettamente pertinenti alle mansioni svolte e per le finalità previste dal titolare del trattamento, sono i seguenti:

- Archivio cartaceo
- Accesso alle cartelle di rete
- Pacchetto Microsoft Office
- Navigazione Internet
- Posta Elettronica
- Gestionale

Modifiche di accesso alle Banche Dati Aziendali
Nel caso in cui Lei dovesse avere l'esigenza di utilizzare una o più banche dati aziendali diverse da quelle sopra selezionate, dovrà far inviare dal proprio diretto Responsabile una richiesta a mezzo e-mail all'ufficio IT precisando la banca dati alla quale si vuole accedere, il tipo di profilo con il quale vuole accedere e la motivazione.
In caso in cui Lei dovesse accorgersi di avere autorizzazioni per accedere ad una o più banche dati aziendali diverse da quelle sopra indicate, dovrà immediatamente darne notizia all'Ufficio IT, che provvederà alle opportune verifiche e correzioni.

Creazione nuove banche dati
Non è permesso realizzare nuove ed autonome banche dati, con finalità diverse da quelle già previste senza preventiva autorizzazione da parte del titolare del trattamento o del delegato privacy interno.

Trattamento dei dati personali
Il trattamento dei dati personali deve essere effettuato esclusivamente in conformità alle finalità previste e dichiarate dall'azienda e, pertanto, in conformità alle informazioni che l'azienda ha comunicato agli interessati. L'eventuale raccolta di dati dovrà avvenire nel rispetto delle procedure e dei modelli di informative e/o moduli per la raccolta del consenso elaborati dall'azienda. L'autorizzato deve prestare particolare attenzione all'esattezza dei dati trattati e provvedere, inoltre, all'aggiornamento degli stessi.

Provvedimenti specifici in materia di trattamento dati personali
In considerazione della sua mansione, il Titolare del trattamento La informa che dovrà rispettare tutti i provvedimenti specifici emanati dalle autorità nazionali e europee in materia di trattamento dati personali.
In particolare, si richiamano le Opinion del WP 29, le Linee guida dei Garanti europei e le Linee guida dell'European Data Protection Board.

Comunicazione e diffusione dei dati
In relazione alle banche dati di cui è autorizzato il trattamento nello svolgimento delle mansioni affidate, ogni ipotesi di comunicazione o, addirittura, di diffusione dei dati a soggetti esterni dovrà essere preventivamente autorizzata di volta in volta dal Titolare del trattamento o dal delegato privacy interno. Gli obblighi relativi alla riservatezza, alla comunicazione ed alla diffusione dei dati dovranno essere osservati anche in seguito a modifica dell'incarico e/o cessazione del rapporto di lavoro.

Trattamenti Cartacei
In base al principio di stretta pertinenza dei trattamenti rispetto alle mansioni svolte, potrebbe dover accedere agli archivi relativi alle banche dati di cui sopra ove necessario per lo svolgimento delle sue mansioni. In tal caso, dovrà chiudere gli archivi alla fine della giornata lavorativa, riponendo le chiavi in apposito contenitore. I documenti (o copia degli stessi) non potranno essere, senza specifica autorizzazione, portati fuori dai luoghi di lavoro, salvo i casi di comunicazione dei dati a terzi preventivamente autorizzati in via generale dall'azienda.
Durante l'utilizzazione, i documenti ed i fascicoli cartacei non devono essere lasciati incustoditi; in caso di assenza temporanea durante l'utilizzo i documenti vanno riposti nei cassetti o armadietti dell'autorizzato. Per l'acceso ai dati particolari al di fuori del normale orario di lavoro dovrà essere chiesta specifica autorizzazione al Responsabile dell'Area.

Misure di sicurezza e Sistemi Informatici, Posta elettronica e Navigazione Internet
Nello svolgimento delle Sue mansioni, è tenuto ad osservare tutte le misure di protezione e sicurezza atti ad evitare rischi di distruzione, perdita, accesso non autorizzato, trattamento non consentito, già predisposte dall'impresa, nonché quelle che in futuro verranno comunicate. Lei dovrà pertanto prendere visione e rispettare il regolamento di utilizzazione di strumenti informatici e le procedure interne (es. Procedura *Data Breach*) adottate dal titolare del trattamento.

Lei è informato sin d'ora che, in caso di anomalie, il personale incaricato del Servizio IT e/o l'amministratore di sistema effettuerà **controlli** anonimi che si concluderanno con avvisi generalizzati diretti ai dipendenti dell'area o del settore in cui è stata rilevata l'anomalia, nei quali si evidenzierà l'utilizzo irregolare degli strumenti aziendali e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite. Controlli su base individuale potranno essere compiuti solo in caso di successive ulteriori anomalie. In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

Luogo, data di emissione della nomina Milano, 15/01/2024

Titolare del trattamento

Luogo e data di firma S. Stefano, 15/01/2024

FIRMA PER PRESA VISIONE

_____