I. Scopo della Policy

La presente policy ha l'obiettivo di fornire istruzioni dettagliate circa le corrette e sicure modalità di consegna a domicilio dei presidi medici effettuate da **Farmaciemorra S.r.l.** (d'ora in avanti la "Società" o il "Titolare del trattamento") a seguito degli ordini ricevuti tramite l'e-commerce del sito web www.farma27.it.

Le implicazioni sulla protezione dei dati personali derivanti da tale attività sono rilevanti ai fini dell'individuazione e della corretta esecuzione delle obbligazioni in materia privacy che incombono sul Titolare del trattamento. Pertanto, il presente documento si pone l'obiettivo di inquadrare le condotte virtuose da assumere al fine di prevenire usi illeciti dei dati personali degli utenti, garantendo loro il rispetto del diritto fondamentale alla protezione dei dati personali.

I documenti e le normative presi in considerazione nella presente policy sono le seguenti:

- **Regolamento UE 2016/679 (GDPR)** del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE;
- **D. Lgs. 196/2003** recante il Codice per la Protezione dei Dati Personali del 30 giugno 2003 e ss.mm.ii.;
- **Provvedimento del Garante della Protezione dei dati personali** "Provvedimento generale rivolto alle aziende sanitarie sulle modalità di consegna dei presidi sanitari al domicilio dell'interessato - 21 novembre 2013 "
- **Provvedimento del Garante della Protezione dei dati personali "**Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario - 7 marzo 2019"

II. Trattamento dei dati personali

A. Finalità e base giuridica del trattamento

I dati personali raccolti dal Titolare sono trattati esclusivamente per **finalità** legate all'erogazione del servizio di consegna a domicilio di presidi medici a seguito degli ordini ricevuti tramite l'e-commerce del sito web www.farma27.it.

La **base giuridica che legittima** il trattamento dei dati personali si rinviene nell'art. 6, par. 1, lett. b) del GDPR, in quanto il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte, ai sensi dell'art. 6, par. 1, lett. c) del GDPR per l'adempimento di obblighi di legge incombenti sul titolare (ad esempio obblighi di natura fiscale derivanti dal servizio erogato) e nell'art. 9, par. 2, lett. h) del GDPR in quanto il trattamento è necessario per finalità di assistenza o terapia sanitaria.

B. Categoria di dati personali

Per le finalità di cui alla lettera **A.** potranno essere raccolte e, successivamente trattate, le seguenti categorie di dati:

- dati anagrafici;
- dati di contatto;
- dati bancari;
- dati sanitari e relativi alla salute (anche se non in modo esplicito, l'acquisto di alcuni presidi medici piuttosto che altri implica la raccolta di informazioni che fanno desumere in via indiretta il possibile stato di salute dell'utente).

C. Periodo di conservazione

Generalmente, in ossequio ai principi di minimizzazione dei dati e di limitazione della conservazione, i dati personali non possono essere conservati più a lungo di quanto necessario al perseguimento delle finalità per le quali essi sono raccolti e trattati, ai sensi dell'articolo 5, paragrafo 1, lettere c) ed e) del GDPR. Pertanto, è necessario comprendere prontamente se sia necessaria o meno l'archiviazione dei dati personali raccolti, rapportando tale necessità alle finalità e al contesto in concreto. Pertanto, I dati dovranno essere conservati in una forma che permetta l'identificazione degli interessati solo per il tempo strettamente necessario al raggiungimento delle finalità per cui i Dati sono stati originariamente raccolti e, in ogni caso, entro i limiti di legge. In particolare, per finalità connesse all'esecuzione del contratto e alla erogazione del servizio richiesto dall'utente, i dati dovranno essere conservati per tutta la durata del rapporto e fino a che sussistano obbligazioni o adempimenti connessi all'esecuzione dello stesso; superato tale termine, in caso di contestazioni e sempre per i dati relativi a servizi richiesti tramite il Sito, alla luce dell'ordinario termine di prescrizione dei diritti (10 anni nell'ordinamento italiano), il periodo di conservazione potrà essere prolungato per ulteriori 11 anni per finalità connesse all'adempimento di obblighi di legge e per consentire a **Farmaciemorra S.r.l.** la difesa dei propri diritti a fronte di possibili contestazioni entro il termine di prescrizione.

D. Destinatari

Per quanto attiene ai soggetti che, verosimilmente, nell'ambito delle attività lavorative possono accedere ai dati personali oggetto di trattamento, è necessario distinguere tra personale interno autorizzato, ditte esterne e autorità competenti. Il Titolare del trattamento, nel caso in cui abbia previsto all'interno della propria organizzazione aziendale un servizio specifico dedicato all'attività in questione (organizzazione degli ordini e

consegna a domicilio) per cui abbia incaricato delle persone e degli asset, nomina tali soggetti quali persone autorizzate per designazione al trattamento ex artt. 29 GDPR e 2-quaterdecies Codice Privacy. Il personale, così individuato, potrà avere accesso ai dati personali e sarà autorizzato a porre in essere le necessarie operazioni di trattamento. Diversamente, l'affidamento a terzi esterni, in particolare dei servizi di consegna a domicilio, comporta per il Titolare l'instaurazione di un apposito rapporto contrattuale da cui discendono obblighi specifici di trattamento dati che dovranno essere minuziosamente descritti all'interno della nomina a responsabile del trattamento ex art. 28 GDPR. Inoltre, I dati personali trattati per le sole finalità sopra esposte potranno essere trasmessi ai soggetti cui la comunicazione è prevista per legge o per regolamento e all'Autorità giudiziaria e/o all'Autorità di Pubblica Sicurezza, nei casi espressamente previsti dalla legge.

E. Diritti dell'interessato

In ogni momento, l'interessato potrà esercitare, ai sensi degli artt. 15-22 del GDPR - ricorrendone i relativi presupposti -, il diritto di:

- chiedere la conferma dell'esistenza o meno di propri dati personali;
- ottenere le indicazioni circa le finalità del trattamento, le categorie dei dati personali, i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati e, quando possibile, il periodo di conservazione;
- chiedere e ottenere la modifica e/o rettifica dei propri dati;
- chiedere e ottenere la cancellazione e/o limitazione del trattamento dei propri dati qualora si tratti di dati o informazioni non necessari – o non più necessari – per le finalità che precedono;
- ottenere la portabilità dei dati, ossia riceverli da un titolare del trattamento, in un formato strutturato, di uso comune e leggibile da dispositivo automatico, e trasmetterli ad un altro titolare del trattamento senza impedimenti, se tecnicamente fattibile;
- opporsi al trattamento in qualsiasi momento nei casi previsti dalla legge.

F. Obblighi informativi del Titolare

L'articolo 13 del GDPR stabilisce l'obbligo per i titolari del trattamento di fornire agli interessati specifiche informazioni al momento della raccolta dei loro dati personali al fine di rendere edotti questi ultimi circa le modalità, la liceità e la correttezza del trattamento.

Sul punto il **Considerando n. 39 GDPR** specifica che:
«Dovrebbero essere **trasparenti** per le persone fisiche le **modalità** con cui sono **raccolti, utilizzati, consultati o altrimenti trattati** dati personali che le riguardano nonché la misura in cui i dati personali sono o saranno trattati. Il principio della trasparenza impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali **siano facilmente accessibili e comprensibili** e che sia utilizzato un **linguaggio semplice e chiaro**».

Farmaciemorra S.r.l. potrà informare gli interessati circa le modalità, la liceità e la correttezza del trattamento con una apposita informativa da prevedere previo acquisto dei prodotti tramite l'e-commerce.

G. Misure di sicurezza tecniche e organizzative

Misure di sicurezza tecniche e organizzative

Come indicato nell'articolo 32, paragrafo 1, GDPR, i Titolari e i Responsabili del trattamento devono adottare misure di sicurezza tecniche e organizzative adeguate al fine di garantire un livello di sicurezza proporzionale ai rischi per i diritti e le libertà delle persone fisiche, derivanti dalla cancellazione accidentale o dolosa, perdita, alterazione, divulgazione non autorizzata o accesso non autorizzato ai dati relativi all'attività trattamentale svolta.
Ai sensi degli articoli 24 e 25 GDPR, inoltre, la Società deve attuare misure tecniche e organizzative per salvaguardare tutti i principi di protezione dei dati personali durante il trattamento e stabilire i mezzi affinché gli interessati possano esercitare i propri diritti.

Data protection by design e by default

Questi principi sottolineano la necessità di tecnologie integrate per il miglioramento della privacy, impostazioni predefinite che riducano al minimo il trattamento dei dati e la fornitura degli strumenti necessari che consentano la massima protezione possibile dei dati personali.

Dal punto di vista tecnico, le specifiche e la progettazione del sistema dovrebbero includere i requisiti per il trattamento dei dati personali in conformità con i principi di cui all'articolo 5 GDPR (liceità del trattamento, finalità e limitazione dei dati, minimizzazione dei dati per impostazione predefinita ai sensi dell'articolo 25, paragrafo 2 GDPR, integrità e riservatezza, responsabilità ecc.).

Il Titolare deve garantire la conformità a questi requisiti applicandoli a tutti i componenti del sistema e a tutti i dati trattati dallo stesso, durante l'intero ciclo di vita, vale a dire durante la memorizzazione (dati a riposo), la trasmissione (dati in transito) e l'elaborazione (dati in uso).

Misure Tecniche

Le misure tecniche si riferiscono agli strumenti e alle tecnologie volti alla protezione fisica dei dati che mitigano i rischi di violazioni dei dati personali (data breach).

Esempi di misure tecniche includono:

1. **Crittografia**: Utilizzo della crittografia per proteggere i dati sia in transito che a riposo.
2. **Firewall e Sistemi di Prevenzione delle Intrusioni (IPS)**: Protezione della rete aziendale da accessi non autorizzati e attacchi.
3. **Autenticazione a più fattori (MFA)**: Aggiunta di livelli di sicurezza nell'accesso ai sistemi e alle informazioni.
4. **Backup e Ripristino dei Dati**: Procedure regolari di backup dei dati e capacità di ripristino in caso di perdita o attacco.

5. **Aggiornamenti e Patch di Sicurezza**: Installazione tempestiva di aggiornamenti software e patch per risolvere vulnerabilità note.

Misure Organizzative

Le misure organizzative si riferiscono alle politiche, procedure e pratiche implementate all'interno di un'organizzazione per garantire la protezione dei dati personali.

Esempi di misure organizzative includono:

1. **Formazione del Personale**: Programmi di formazione e sensibilizzazione per i dipendenti sulle pratiche di sicurezza e protezione dei dati.
2. **Politiche di Sicurezza dei Dati**: Definizione e implementazione di politiche aziendali per la gestione e protezione dei dati personali.
3. **Controlli degli Accessi**: Procedure per limitare l'accesso ai dati personali solo a personale autorizzato.

Misure organizzative da Rispettare per la Consegna di Farmaci a Domicilio

1. Luogo e Orari di Consegna
    - **Scelta del Luogo e degli Orari:** La consegna dei farmaci deve avvenire nel luogo indicato dall'interessato, rispettando gli orari scelti da quest'ultimo tra quelli proposti dal titolare o dal responsabile del trattamento.

      È fondamentale rispettare le preferenze temporali dell'interessato per garantire che la consegna avvenga in modo discreto e sicuro.
    - **Consegna Diretta:** Preferibilmente, la consegna deve avvenire nelle mani dell'interessato. È **altamente sconsigliato** lasciare i presidi medici incustoditi nelle vicinanze del luogo di consegna per evitare il rischio di accessi non autorizzati e per tutelare i diritti e le libertà dell'interessato.

2. Imballaggio dei Farmaci
    - **Contenitore Non Trasparente:** I farmaci devono essere imballati in contenitori non trasparenti, indipendentemente dalle loro dimensioni e natura. Questo è essenziale per impedire che terzi possano identificare il contenuto del pacco.
    - **Assenza di Indicazioni Esterne:** L'imballaggio esterno non deve riportare indicazioni sul contenuto del pacco, in modo da non ledere il diritto alla protezione dei dati personali dell'interessato e ridurre il rischio di conseguenze indesiderate come discriminazioni o imbarazzo.
3. Consegna a Terzi Delegati
    - **Espressa delega dell'Interessato:** I farmaci possono essere consegnati a terzi, come vicini di casa, parenti o portieri, solo se l'interessato ha fornito un'esplicita delega nei confronti di tali soggetti. È importante che la delega sia chiara e documentata per evitare malintesi e garantire la correttezza della consegna.
4. Gestione delle Mancate Consegne
    - **Avviso di Consegna:** Nel caso in cui né l'interessato né il terzo delegato siano presenti al momento della consegna, il personale incaricato deve lasciare esclusivamente un avviso di tentata consegna. L'avviso non deve contenere indicazioni sulla tipologia dei presidi medici, al fine di tutelare la riservatezza dell'interessato.
5. Identificazione del Personale di Consegna
    - **Divise e Automezzi:** Il personale addetto alla consegna non deve indossare divise o utilizzare automezzi che riportino scritte identificative della Società o della specifica tipologia dei presidi consegnati . Questo per evitare di rivelare informazioni a terzi non autorizzati e per proteggere i diritti e le libertà degli interessati.

L'adozione delle suddette misure è essenziale per garantire la riservatezza, l'integrità e la disponibilità dei dati personali degli interessati. Tali pratiche, se correttamente implementate, contribuiranno a rispettare le normative vigenti in materia di protezione dei dati personali, evitando possibili violazioni e sanzioni.

A. Sanzioni

In particolare, deve essere chiarito, nell'ambito della presente politica aziendale, che qualora il trattamento dei dati personali sia contrario al dettato normativo, provocando una violazione dei dati personali, il Titolare del trattamento sarà direttamente responsabile.

Art. 82 GDPR

È rubricato «Diritto al risarcimento e responsabilità».

Stabilisce come il Titolare risponderà per il danno cagionato.

Art. 83 GDPR

È rubricato «Condizioni generali per infliggere sanzioni amministrative pecuniarie». Individua le condizioni generali per l'irrogazione delle sanzioni amministrative pecuniarie.

Art. 84 GDPR

È rubricato «Sanzioni». Rimanda alla normativa del Codice Privacy per quanto riguarda la responsabilità penale.

L'art. 83, par. 4, lett. a) prevede sanzioni fino a 10 mln di euro o, per le imprese, del 2% del fatturato annuo qualora sia accertata la violazione da parte del Titolare degli obblighi derivanti dagli artt. 8, 11, da 25 a 39, 42 e 43 GDPR.

L'art. 83, par. 4, lett. a) prevede sanzioni fino a 20 mln di euro o, per le imprese, del 2% del fatturato annuo qualora sia accertata la violazione da parte del Titolare dei principi base del trattamento ai sensi degli artt. 5, 6, 7 e 9 GDPR.

III. REVISIONE DELLA PRESENTE POLICY

È opportuno revisionare la presente policy annualmente.

N.B.

La presente Policy Privacy è destinata esclusivamente per scopi aziendali interni. È vietata la divulgazione, riproduzione o distribuzione, totale o parziale, senza la previa autorizzazione scritta della Società di consulenza legale **Studio Themis S.r.l.** con sede legale in Largo Parrocchia n.1, Palma Campania (NA).