Capannori Servizi S.r.l. – a socio unico
Società soggetta a direzione e coordinamento dell'Ente Comune di Capannori

Sede legale: Via del Parco, 5 – Frazione Marlia - 55014 – Capannori (LU)
C.F./P.Iva: 02042140463 R.E.A. CCIAA LU - 192019 - Capitale sociale € 200.000,00 i.v.
Tel: 0583/307556 Sito Web: http://www.capannoriservizi.t
E-mail Pec: capannoriservizisrl@cgn.legalmail.it
E-mail: direzione@capannoriservizi.it E-mail: rsadongori@capannoriservizi.it

Regolamento privacy

Regolamento interno per la protezione dei dati personali

INDICE

1.Introduzione

Il diritto alla privacy è un vero e proprio diritto inviolabile della persona che non si limita alla tutela della riservatezza o alla protezione dei dati, ma implica il pieno rispetto dei diritti e delle libertà fondamentali, nonché della dignità. Per questi motivi la cultura della privacy necessita di crescere e rafforzarsi, principalmente fra gli operatori della sanità, perché solo con la conoscenza minima dei principi fondamentali che stanno alla base della vigente normativa, potranno essere adottati correttamente tutti gli adempimenti di legge, nel trattamento di dati di competenza, con la consapevolezza di non affrontare un inutile gravame, bensì di contribuire concretamente al miglioramento della qualità del rapporto con l'utente.

2.Scopo

Il presente documento è uno strumento di applicazione del Regolamento UE 2016/679 (*General data Protection Regulation* - GDPR -) e del D.Lgs. n. 196/2003 nell'ambito dell'organizzazione aziendale, frutto di un'attenta analisi delle problematiche concrete che quotidianamente emergono nella tutela della riservatezza dei dati personali. La stesura del Regolamento nasce, infatti, dall'esigenza di regolamentare la disciplina in argomento all'interno della società al fine di recepire i principi fondamentali della nuova normativa, individuare e definire i ruoli e le figure coinvolte nei processi di gestione dei trattamenti sopra citati e porre in essere tutte le misure tecnico-organizzative previste. Il documento è inoltre espressione del c.d. principio di *accountability* (ossia di responsabilizzazione), che rappresenta la base sulla quale è stato costruito il Regolamento europeo: tale principio impone di scegliere le misure di sicurezza adeguate in base al contesto operativo.

3.Campo di applicazione

La normativa ha ben definito la gerarchia in materia di gestione della privacy, prevedendo, infatti, le figure fondamentali da individuare all'interno delle singole Aziende:

- Titolare: la persona fisica, la persona giuridica, la Pubblica Amministrazione e qualsiasi altro Ente, Associazione o Organismo cui competono, anche unitamente ad altro Titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.
- Responsabile: la persona fisica, la persona giuridica, la Pubblica Amministrazione e qualsiasi altro Ente, Associazione o Organismo preposti dal Titolare al trattamento di dati personali.
- Incaricato/Autorizzato: la persona fisica autorizzata dal Titolare o dal Responsabile a compiere operazioni di trattamento.

L'impianto organizzativo sopra descritto risulta ormai consolidato e funzionale alla gestione della protezione dei dati personali presso la società.

Il Legislatore europeo, definiti il perimetro di azione, le figure coinvolte e i nuovi concetti finalizzati al corretto trattamento dei dati personali e della tutela delle persone fisiche, consente, in piena autonomia, di organizzarsi al fine di ottemperare agli obblighi previsti.

4.Le figure coinvolte

Le figure coinvolte nei processi di trattamento dei dati personali sono descritte nei seguenti paragrafi.

4.1Titolare Il Titolare del trattamento è "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; Il Titolare del trattamento di tutti i dati personali è considerata la società (Capannori Servizi S.r.l. – a socio unico), rappresentata dal suo Legale Rappresentante *pro tempore*.

4.2 Compiti e Responsabilità

Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 del Regolamento UE:

- liceità, correttezza e trasparenza;
- limitazione della finalità;
- minimizzazione dei dati;
- esattezza dei dati;
- limitazione della conservazione;

- integrità e riservatezza.

Il Titolare deve mettere in atto le misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme alla normativa in vigore. Tali misure sono definite fin dalla fase di progettazione e messe in atto per applicare in modo efficace i principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato.
Il Titolare deve in particolare fornire all'interessato le informazioni relative al trattamento dei dati che lo riguardano.
4.3 Responsabile della Protezione dei dati (DPO/RPD) Il Regolamento UE introduce, all'art. 37, una nuova figura, reclutata in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere ai compiti assegnati. Il Titolare ha provveduto a designare tale soggetto, il quale è contattabile al seguente indirizzo di posta elettronica: marcucci.a85@yahoo.com.
I dati di contatto del RPD sono esplicitati nelle informative sul trattamento dei dati personali in uso.
4.4 Compiti e Responsabilità Il Responsabile della protezione dei dati svolge i seguenti compiti:
- informare e fornire consulenza al Titolare nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dalla normativa in materia di protezione dei dati. In tal senso può indicare al Titolare del trattamento i settori funzionali ai quali riservare degli audit interno in tema di protezione dei dati, le attività di formazione interna per il personale che tratta dati personali e a quali trattamenti dedicare maggiori risorse ed attenzione in relazione al rischio riscontrato;
- sorvegliare l'osservanza della normativa relativa alla protezione dei dati, fermo restando le responsabilità del Titolare del trattamento. Fanno parte di questi compiti la raccolta di informazioni per individuare i trattamenti svolti, l'analisi e la verifica dei trattamenti in termini della loro conformità, l'attività di informazione, consulenza e indirizzo nei confronti del Titolare;
- sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare del trattamento;
- fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento;
- cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 Regolamento UE;
- effettuare, se del caso, consultazioni relativamente a ogni altra questione purché si assicuri l'assenza di conflitto di interesse.
La figura del Responsabile della protezione dei dati, infatti, è incompatibile con chi determina le finalità o i mezzi del trattamento, tra cui il Responsabile del Servizio di Protezione e Prevenzione, dell'Anticorruzione e Trasparenza, dei Sistemi informativi e/o di qualunque incarico o funzione che comporta la determinazione di finalità o mezzi del trattamento. Il Titolare assicura che il Responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. A tal fine il Responsabile della protezione dei dati deve: - essere invitato a partecipare alle riunioni di coordinamento dei Dirigenti/Responsabili che abbiano per oggetto questioni inerenti la protezione dei dati personali; - disporre tempestivamente di tutte le informazioni pertinenti le decisioni che impattano sulla protezione dei dati, in modo da poter rendere una consulenza idonea; - essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente, o in caso di verifiche da parte di qualsivoglia Autorità.
Il RPD opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti; in particolare, non deve ricevere istruzioni in merito al loro svolgimento né sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati, non può essere rimosso o penalizzato dal Titolare per l'adempimento dei propri compiti. Ferma restando l'indipendenza nello svolgimento di detti compiti, il RPD riferisce direttamente al Titolare. Nel caso in cui siano rilevate dal RPD o sottoposte alla sua attenzione decisioni incompatibili con il Regolamento UE e con le indicazioni fornite dallo stesso RPD, quest'ultimo è tenuto a manifestare il proprio dissenso, comunicandolo al

Titolare ed al Responsabile del trattamento. Compiti del Responsabile della Sicurezza sono quelli di costituire lo strumento di pianificazione e controllo della politica della sicurezza di dati e banche di dati, tesa a garantire la loro integrità, riservatezza e disponibilità.

4.5 Referente interno Poiché l'organizzazione interna non risulta particolarmente complessa e l'art. 29 D.Lgs. n. 196/2003 è stato abrogato, non è stata nominata uno specifico responsabile interno. Di fatto il referente interno è il Legale Rappresentante che provvede a coinvolgere il DPO tutte le volte in cui emergono dubbi o problematiche legate alla materia in oggetto.

4.6 Incaricato Il Titolare del trattamento ha individuato gli incaricati al trattamento intesi come persone fisiche autorizzate a compiere operazioni di trattamento dati. Gli incaricati al trattamento dei dati all'interno della società sono tutti coloro che quotidianamente gestiscono i dati, sia su supporto cartaceo che informatico. Essi devono elaborare i dati personali ai quali hanno accesso attenendosi alle istruzioni del Titolare e del DPO/RPD, della natura e finalità dei trattamenti svolti, delle tipologie di dati personali oggetto di trattamento e delle misure tecnico organizzative attuate per la corretta protezione dei dati personali.

5. Trattamento dei dati

Ai sensi del c. 2 dell'art. 4 del Regolamento UE, con il termine "trattamento", si intende: "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" Ai sensi dell'art. 5 del Regolamento UE, presso la società i dati personali saranno:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non siano incompatibili con tali finalità;

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per i quali sono trattati;

d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;

e) conservati per l'arco temporale previsto dalla tipologia di attività per la quale sono richiesti.

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, distruzione o danno accidentale.

6. Sicurezza del trattamento

Ai sensi dell'art. 32 del citato regolamento UE il Titolare ha l'obbligo di mettere in atto tutte le misure tecniche ed organizzative atte a garantire un livello di sicurezza adeguato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura del campo di applicazione, 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. Le misure tecniche ed organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento sono, tra le altre, la minimizzazione dei dati personali, la capacità di assicurare la continua riservatezza, integrità, disponibilità e la resilienza dei sistemi e dei servizi che trattano i dati personali nonché la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico. La società ha adottato le seguenti misure tecnico-organizzative:

- sistemi di autenticazione: il trattamento di dati personali con strumenti elettronici è consentito esclusivamente al personale autorizzato e dotato di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento, o ad un insieme di trattamenti. Le credenziali di autenticazione consistono in un codice identificativo associato ad una password composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito. La password non deve contenere riferimenti agevolmente riconducibili all'operatore e deve essere modificata, oltre che al primo accesso, successivamente, almeno ogni 3/6 mesi a seconda delle tipologie di dati trattati.

- sistemi di autorizzazione: i profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento. Periodicamente viene verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione;
- sistemi di protezione (antivirus; firewall; antintrusione; anti-malware; anti-spam);
- misure antincendio;
- porte, armadi e contenitori dotati di serrature e/o ignifughi;
- sistemi di backup e conservazione di archivi elettronici.

La conformità del trattamento dei dati al Regolamento UE in materia di protezione dei dati personali è dimostrata, pertanto, attraverso l'adozione delle misure di sicurezza adeguate.

7. Dati trattati

Nell'esercizio delle proprie funzioni istituzionali la società tratta le seguenti categorie di dati:
- **Dati personali:** "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"(art. 4 c. 1);
- **Dati relativi alla salute:** i dati personali attinenti alla salute fisica o mentale di una persona fisica.

8. Informativa

In ottemperanza ai disposti della normativa vigente in materia di privacy, l'Azienda ha provveduto a rivedere le informative rese ai vari interessati. L'informativa è fornita per iscritto, attraverso cartelli affissi nei locali di accesso dell'utenza e agevolmente visibili dal pubblico. Quando possibile viene fatta sottoscrivere. L'informativa contiene:
- l'identità e i dati di contatto del Titolare del trattamento;
- i dati di contatto del Responsabile della protezione dei dati;
- le finalità e le modalità del trattamento cui sono destinati i dati personali;
- le categorie dei dati trattati;
- i destinatari dei dati;
- il periodo di conservazione;
- la base giuridica;
- i diritti dell'interessato.

9. Diritti dell'interessato

Il Titolare del trattamento deve adottare, tra le altre, le misure tecniche ed organizzative eventualmente necessarie per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati, che dovrà avere per impostazione predefinita forma scritta (anche elettronica).
Ai sensi degli artt. 15-22 del Regolamento UE, nei limiti consentiti dalla normativa, l'interessato ha il diritto di chiedere al Titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano, chiedere la rettifica o la cancellazione dei dati, chiedere la limitazione del trattamento, ricevere in un formato strutturato di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano, opporsi al trattamento, proporre reclamo all'Autorità di controllo.

10. Violazione dei dati

Per violazione dei dati personali, di seguito data breach, si intende la violazione di sicurezza che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dal Titolare. I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 del Regolamento UE, sono di seguito indicati:
- danni fisici, materiali o immateriali alle persone fisiche;

- perdita del controllo dei dati personali;
- limitazione dei diritti, discriminazione;
- furto o usurpazione d'identità;
- perdite finanziarie, danno economico o sociale;
- pregiudizio alla reputazione;
- perdita di riservatezza dei dati personali protetti da segreto professionale.

Qualora il Titolare dovesse ritenere che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata sia elevato, deve informare questi ultimi (art. 34 del Regolamento UE).
Il rischio per i diritti e le libertà degli interessati può essere considerato:
- alto: quando la violazione può, a titolo esemplificativo, coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati, riguardare categorie particolari di dati personali, comprendere dati che possono accrescere ulteriormente i potenziali rischi (dati di localizzazione, finanziari, relativi alle abitudini e preferenze) e i rischi imminenti e con un'elevata probabilità di accadimento impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (persone fragili, minori, soggetti indagati ecc.);
- medio: quando gli interessati potrebbero incontrare conseguenze che dovrebbero essere in grado di superare anche con alcune difficoltà, come, a titolo esemplificativo danni alla proprietà, citazione in giudizio, peggioramento della salute, ecc.;
- basso: quando gli interessati potrebbero incontrare alcuni disagi, che sarebbero in grado di superare con difficoltà limitate, eventuali ritardi di accesso ai servizi aziendali, stress, ecc.;
- trascurabile: nel caso in cui gli interessati non sarebbero danneggiati o potrebbero incontrare alcuni inconvenienti.

Il Titolare, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, deve provvedere, in ottemperanza all'art. 33 del Regolamento UE, alla notifica al Garante per la protezione dei dati, entro 72 ore dal momento in cui ne è venuto a conoscenza. Chiunque (Referente interno e/o incaricati) venga a conoscenza di eventuali violazioni è tenuto ad informare tempestivamente il Titolare ed il Responsabile della protezione dei dati. Il Titolare, pertanto, provvederà ad informare tutti gli incaricati e a denunciare tempestivamente al Responsabile della protezione dei dati, eventuali casi di violazioni. La notifica, sia all'Autorità Garante che all'interessato, deve contenere almeno gli elementi minimi previsti rispettivamente dagli artt. 33 e 34 del Regolamento UE. Il Titolare deve opportunamente documentare tutte le violazioni di dati personali subite, anche se non comunicate alle Autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio. Tale documentazione deve essere conservata con la massima cura e diligenza in quanto può essere richiesta dal Garante privacy al fine di verificare il rispetto delle disposizioni del Regolamento UE.

11. Disposizioni finali.

Per tutto quanto non espressamente disciplinato nel presente Regolamento, si applicano le disposizioni del Regolamento UE e tutte le sue norme attuative vigenti.

Ultima revisione 30 dicembre 2023