SRR
trapani provincia sud

Regolamento per la gestione della riservatezza e protezione dei dati personali

(approvato giusta deliberazione del CdA di cui al verbale di adunanza del 22.09.2023)

S.R.R. Trapani Provincia Sud
Società Consortile per azioni
Corso Vittorio Emanuele n°168/C
91028 Partanna TP

C.F. | P.I. 02485430819

Tel. (+39) 0924-203285

srrtrapanisud@pec.it
info@srrtrapaniprovinciasud.it
Sito internet: www.srrtrapaniprovinciasud.it

Sommario

S.R.R. Trapani Provincia Sud Soc. Consortile s.p.a.

Art. 1 - Oggetto del regolamento

1. Il presente regolamento disciplina il trattamento dei dati personali contenuti nelle banche dati organizzate, gestite e/o utilizzate dalla **SRR Trapani Provincia Sud S.C.p.A.** (*d'ora innanzi anche solo* **"ente"** o **"SRR"**) in relazione allo svolgimento delle proprie finalità istituzionali, in attuazione:
   - della normativa in materia di diritto di accesso documentale, accesso civico e accesso generalizzato;
   - del Regolamento UE 2016/679 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;
   - della normativa nazionale in materia vigente e all'uopo applicabile.

Art. 2 - Finalità

1. La SRR, nell'assolvimento delle proprie finalità istituzionali, secondo i principi generali di liceità, correttezza e trasparenza, garantisce che il trattamento dei dati personali si svolga con modalità che assicurino il pieno rispetto del diritto alla riservatezza ed all'identità personale, nonché nel pieno rispetto delle norme vigenti in materia di protezione e gestione dei dati personali.

2. In adempimento dell'obbligo di comunicazione interna ed esterna e di semplificazione dell'azione amministrativa, la SRR favorisce la trasmissione di dati e documenti tra le banche dati e gli archivi in uso alla stessa, degli enti territoriali, degli enti pubblici, dei gestori e degli incaricati di pubblico servizio, operanti nell'ambito dell'Unione Europea.

3. La trasmissione dei dati può avvenire anche attraverso l'utilizzo di sistemi informatici e telematici, reti civiche e reti di trasmissione di dati ad alta velocità;

4. Ai fini del presente regolamento, per finalità istituzionali della SRR si intendono le funzioni ad essa stessa attribuite dalle leggi, dallo statuto e dai regolamenti applicabili o per effetto di accordi, intese e/o convenzioni.

5. I trattamenti sono compiuti dalla SRR per le seguenti finalità:

a) per l'esecuzione di un adempimento di interesse pubblico o connesso all'esercizio di pubblici poteri e/o attività equiparate. In particolare, a titolo esemplificativo, rientrano in questo ambito i trattamenti compiuti per:

- l'esercizio delle funzioni tecnico-amministrative che riguardano le attività di regolamentazione del servizio di gestione dei rifiuti nell'ambito territoriale di relativa competenza e, precisamente, tutte quelle attività afferenti ai settori organici dei servizi di gestione delle risorse umane, di approvvigionamento, di vigilanza ed ispezione, di pianificazione e governo del territorio, di coordinamento dei servizi, di info-sensibilizzazione dell'utenza nonché di sviluppo e innovazione; - la gestione dei servizi di statistica;

S.R.R. Trapani Provincia Sud

- l'esercizio di ulteriori funzioni tecnico-amministrative per lo svolgimento dei servizi di competenza di altri enti coinvolti nell'esercizio associato della gestione integrata dei ciclo dei rifiuti urbani ed assimilati, affidate alla SRR in base alla vigente legislazione e/o sulla scorta di appositi accordi, intese o convenzioni.

b) per l'adempimento di un obbligo legale al quale è soggetta la SRR. In tal caso, la specifica finalità del trattamento è stabilita dalla fonte normativa che lo disciplina;

c) per l'esecuzione di un contratto con soggetti interessati;

d) per assolvere gli obblighi ed esercitare i diritti specifici della SRR o dell'interessato in materia di diritto del lavoro e della sicurezza e protezione sociale;

e) per accertare, esercitare o difendere un diritto in sede giudiziaria;

f) per finalità di medicina preventiva o di medicina del lavoro e valutazione della capacità lavorativa dei propri dipendenti;

g) per le specifiche finalità diverse da quelle di cui alle precedenti lettere, purché l'interessato esprima il suo libero ed incondizionato consenso al trattamento.

Art. 3 – Definizioni

1. Ai fini del presente regolamento si intende per:

a) "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;

b) "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 ad uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

c) "Dati identificativi": i dati personali che permettono l'identificazione diretta dell'interessato;

d) "Dati particolari e giudiziari": dati che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, nonché la trattazione di dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona. *(cfr.* **ALLEGATO n. 1**, *contenente i tipi di dati particolari e giudiziari per cui è consentito il relativo trattamento, nonché le operazioni eseguibili)*;

S.R.R. Trapani Provincia Sud Società Consortile per azioni

e) "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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

f) "Referente Privacy": la persona fisica delegata alla gestione interna delle policy di privacy e del Registro dei Trattamenti, che svolge funzioni di direzione, impulso e controllo sui trattamenti dei dati personali, nonché di coordinamento e sovraintendimento generale per l'Area funzionale a cui è assegnata, tenendo anche i rapporti con il Responsabile della Protezione dei Dati (DPO);

g) "Responsabile della Protezione dei Dati (DPO)": la persona fisica individuata come Responsabile della protezione dei dati personali ai sensi del GDPR *(in particolare ex artt. 37, 38, 39);*

h) "Designato al trattamento (responsabile interno)": la persona fisica che, secondo l'assetto organizzativo dell'Ente ed il livello di autorizzazione conseguentemente accordatosi, ricopre un ruolo gestionale e di responsabilità all'interno dell'Ente stesso, determinando (in conformità al Regolamento interno, alle procedure e direttive generali) specifiche modalità operative ed organizzative rispetto ad uno o più trattamenti ricadenti nella sfera di propria diretta competenza;

i) "Autorizzato al trattamento": la persona fisica, espressamente designata, che opera sotto l'autorità ed il modello organizzativo adottato da parte del titolare del trattamento, con specifici compiti e funzioni connessi al trattamento dei dati personali;

j) "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 *[cfr. art. 4, comma 5, lett.ra d)].*

k) "Interessato": la persona fisica, cui si riferiscono i dati personali;

l) "Consenso dell'interessato": qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

m) "Dato anonimo": il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

n) "Blocco": la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;

o) "Banca dati": qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;

p) "Garante": l'autorità preposta al controllo della privacy;

S.R.R. Trapani Provincia Sud
Società Consortile per azioni
Corso Vittorio Emanuele n°168/C
91028 Partanna TP
C.F. | P.I. 02485430819
Tel. (+39) 0924-203285
srrtrapanisud@pec.it
info@srrtrapaniprovinciasud.it
Sito internet: www.srrtrapaniprovinciasud.it

q) "Violazione di dati personali": violazione della sicurezza che comporta anche accidentalmente la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque elaborati nel contesto della fornitura di un servizio di comunicazione accessibile al pubblico;

r) "Profilazione": qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

s) "Pseudonimizzazione": il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.

Art. 4 – Soggetti

1. La SRR rappresentata, in ossequio al Regolamento UE 2016/679 e dal proprio Statuto, dal Presidente del Consiglio di Amministrazione pro-tempore in carica, è il Titolare del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee (di seguito indicato con "*Titolare*"). Il Presidente può delegare le relative funzioni ad un dirigente/responsabile di servizio in possesso di adeguate competenze.

2. Il Titolare è responsabile del rispetto dei principi contenuti nell'art. 5 del Regolamento UE 2016/679**: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.**

3. Il Titolare adotta misure appropriate per fornire all'interessato:

a) **le informazioni indicate dall'art. 13 del Regolamento UE 2016/679, qualora i dati personali siano raccolti presso lo stesso interessato;**

b) **le informazioni indicate dall'art. 14 del Regolamento UE 2016/679, qualora i dati personali non stati ottenuti presso lo stesso interessato.**

4. Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare deve effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito indicata con *"DPIA"*) ai sensi dell'art. 35, del Reg. citato, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento, tenuto conto di quanto indicato dal successivo art. 8.

5. Il Titolare, inoltre, provvede a:

a) **nominare dei propri <u>Referenti Generali</u> nelle persone dei Dirigenti delle Aree funzionali in cui si articola la struttura organizzativa dell'ente, i quali sono preposti alla direzione, al coordinamento e controllo apicale delle operazioni di trattamento dei dati contenuti nelle banche dati esistenti nelle unità organizzative di loro competenza, alla gestione interna delle policy di privacy (*proposte di stesura di procedure/istruzioni/indicazioni et similia sulla privacy e sul trattamento dati)* e del Registro dei Trattamenti, nonché al raccordo tra la propria struttura ed il Titolare ovvero il DPO. Per il trattamento di dati, il titolare può avvalersi anche di soggetti pubblici o privati;**

b) **nominare appositi soggetti Designati al trattamento (Responsabile interno) nelle persone dei Capi Servizio incardinati nella struttura organizzativa dell'Ente i quali, secondo l'assetto organizzativo dell'Ente stesso ed il livello di autorizzazione conseguentemente accordatosi, ricoprono un ruolo gestionale e di responsabilità all'interno dell'Ente medesimo, essendo preposti al sovraintendimento e al coordinamento del trattamento dei dati contenuti nelle banche dati esistenti nei Settori e negli Uffici di loro stretta competenza, nonché alla funzione di raccordo tra il Servizio di propria afferenza e l'Area funzionale di loro rispettiva appartenenza;**

c) **nominare il Responsabile della protezione dei dati (DPO);**

d) **nominare quale Responsabile del trattamento i soggetti pubblici o privati affidatari di attività e servizi per conto della SRR, relativamente alla gestione di banche dati esterne all'ente stesso in virtù di convenzioni, di contratti o di incarichi professionali o altri strumenti giuridici consentiti dalla legge, per la realizzazione di attività connesse all'esercizio delle attività istituzionali della SRR (*Consulenti, Fornitori et similia*);**

e) **nominare un Amministratore di sistema/Responsabile dei servizi informativi a cui spetta il compito di supportare il Titolare e/o il Responsabile del trattamento nel mettere in atto le misure tecniche per garantire un livello di sicurezza adeguato al rischio (*cfr. art. 32 del Regolamento UE 27 aprile 2016 n. 679).***

6. Il Responsabile del trattamento, designato mediante determinazione del Presidente del CdA, provvede, per il proprio ambito di competenza, a tutte le attività previste dalla legge e a tutti i compiti affidatigli dal Titolare, analiticamente specificati per iscritto nell'atto di designazione ed, in particolare, a:

a) **tenere il registro delle categorie di attività di trattamento svolte per conto del Titolare;**

b) **adottare idonee misure tecniche e organizzative adeguate per garantire la sicurezza dei trattamenti;**

c) **assistere il Titolare nella conduzione della valutazione dell'impatto sulla protezione dei dati fornendo allo stesso ogni informazione di cui è in possesso;**

S.R.R. Trapani Provincia Sud
Società Consortile per azioni
Corso Vittorio Emanuele n°168/C
91028 Partanna TP
C.F. | P.I. 02485430819
Tel. (+39) 0924-203285
srrtrapanisud@pec.it
info@srrtrapaniprovinciasud.it
Sito internet: www.srrtrapaniprovinciasud.it

d) **informare il Titolare, senza ingiustificato ritardo, della conoscenza di casi di violazione dei dati personali c.d. "data breach", per la successiva notifica della violazione al Garante Privacy, nel caso che il Titolare stesso ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati.**

Art. 5 - Responsabile della protezione dei dati

1. Il Presidente del CdA, con suo formale provvedimento, nomina il Responsabile della Protezione dei Dati, in funzione delle sue qualità professionali ed, in particolare, della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati personali nonché della capacità di assolvere i compiti di controllo a lui affidati.

2. Il Responsabile della protezione dei dati può essere un dirigente o funzionario in posizione apicale, oppure, un incaricato esterno che potrà assolvere ai propri compiti in base ad un contratto pubblico di servizio.

3. L'atto di nomina ed i dati di contatto del Responsabile della protezione dei dati sono pubblicati sul sito istituzionale della SRR nella pertinente sezione "*Amministrazione trasparente*" e comunicati al Garante della protezione dei dati personali.

4. Il Responsabile della protezione dei dati deve essere tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali e gli vanno fornite le risorse necessarie per assolvere a tali compiti, accedere ai dati personali, ai trattamenti e per mantenere costantemente ed adeguatamente aggiornata la propria conoscenza specialistica.

5. Non può essere rimosso o penalizzato a causa dell'adempimento dei propri compiti. Riferisce e dipende direttamente dal Presidente del CdA.

6. Gli interessati possono contattare il Responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento.

7. Il Responsabile della protezione dei dati è tenuto al segreto e alla riservatezza in merito all'adempimento dei propri compiti ed, in conformità al diritto dell'Unione o degli Stati membri, deve svolgere almeno le seguenti funzioni:

a) **sorvegliare sull'osservanza del presente regolamento nonché della normativa nazionale e comunitaria in materia vigente ed applicabile da parte dei titolari del trattamento e dei responsabili del trattamento, comprese le attribuzioni loro riservate in ordine alla responsabilità, alla sensibilizzazione e alla formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;**

b) **fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento congiuntamente ai Responsabili del trattamento;**

c) **cooperare con l'Autorità garante per la protezione dei dati personali e fungere da punto di contatto per questioni connesse al trattamento dei dati personali;**

d) **informare e fornire consulenza all'Assemblea soci, al Consiglio di Amministrazione, al Presidente, ai Dirigenti e a tutte le unità organizzative aziendali in merito agli obblighi derivanti dal presente regolamento nonché dalla normativa nazionale e comunitaria protempore vigente in materia di gestione e protezione dei dati personali;**

8. In caso di affidamento dell'incarico a soggetto terzo, i compiti attribuiti al DPO sono puntualmente indicati nell'apposito contratto di servizio.

Art. 6 - Trattamento dei dati personali

1. Le disposizioni del presente regolamento si intendono riferite al trattamento, alla diffusione e alla comunicazione dei dati all'esterno. L'accesso ai dati personali da parte delle strutture e dei dipendenti della SRR - comunque limitato ai casi in cui sia finalizzato al perseguimento dei fini istituzionali - è ispirato al principio della circolazione delle informazioni, secondo il quale la SRR provvede alla organizzazione delle informazioni e dei dati a sua disposizione mediante strumenti, anche di carattere informatico, atti a facilitare l'accesso e la fruizione, anche presso le strutture dipendenti.

2. Ogni richiesta di accesso ai dati personali da parte delle strutture e dei dipendenti, debitamente motivata, deve essere soddisfatta nella misura necessaria al perseguimento dell'interesse istituzionale e ai diritti degli interessati.

3. Il responsabile della banca dati, specie se la comunicazione concerne dati particolari, può tuttavia disporre, con adeguata motivazione, le misure ritenute necessarie alla tutela della riservatezza delle persone.

Art. 7 – Coordinamento con amministrazione trasparente, procedimenti di accesso civico, generalizzato e documentale

1. Costituisce onere sia del **Responsabile della protezione dei dati personali** che del **Responsabile per la prevenzione della corruzione e della trasparenza**, nel caso in cui siano incaricati due soggetti diversi, coordinare la loro attività al fine di semplificare e minimizzare l'impatto degli adempimenti sull'attività degli uffici e garantire la massima protezione dei dati personali ogniqualvolta procedimenti di ufficio o attivati su istanza di soggetti esterni comportino attività di pubblicazione dei dati personali in amministrazione trasparente, il rilascio di dati personali in occasione di istanze di accesso civico, generalizzato e documentale.

2. In tali ultime ipotesi dovranno essere adottate misure di sicurezza adeguate compresa la pseudonimizzazione, la minimizzazione e la cifratura dei dati personali.

Art. 8 - Formazione del personale

1. Costituisce onere sia del **Responsabile della protezione dei dati personali** che del **Responsabile per la prevenzione della corruzione e della trasparenza**, nel caso in cui siano incaricati due soggetti diversi, coordinare la loro attività onde attuare misure di formazione del personale, anche con riscontro dell'acquisizione di abilità e competenze, al fine di garantire, nell'attività degli uffici, il rispetto delle norme in materia di trasparenza e l'assolvimento degli adempimenti atti a tutelare i diritti di riservatezza dei dati personali degli interessati e dei dipendenti.

Art. 9 – Trattamenti consentiti

1. La SRR, di norma, essendo per sua natura giuridica tenuta ad osservare la disciplina sulla Privacy applicabile ai soggetti pubblici, non è tenuta a chiedere il consenso al trattamento dei dati da parte degli interessati.

2. La pubblicazione e la divulgazione di atti e documenti che determinano una "*diffusione*" dei dati personali, comportando la conoscenza dei dati da parte di un numero indeterminato di soggetti, è legittima solo se la diffusione è prevista da una norma di legge o di regolamento.

3. Prima della pubblicazione di dati personali deve essere valutato se le finalità di trasparenza e di comunicazione possono essere perseguite senza divulgare dati personali.

4. Se risulta possibile occorre citare i dati personali solo negli atti a disposizione degli uffici, richiamati quale presupposto dei provvedimenti di rito e consultabili solo da interessati e controinteressati, oppure utilizzare espressioni di carattere generale, soprattutto nel quadro di attività particolarmente sensibili (*Procedure d'affidamento, Atti contenenti dati personali dei dipendenti in forza, ecc...*).

5. Deve essere valutato anche la possibilità di rendere pubblici atti e documenti senza indicare i dati che portino, direttamente o indirettamente, all'identificazione degli interessati.

6. Per attività di comunicazione istituzionale che contemplino l'utilizzo di dati personali, andrà posta particolare attenzione alla necessità di fornire un'adeguata informativa relativa al trattamento e, soprattutto, andrà valutato se risulti necessaria l'acquisizione, anche successiva, del consenso al trattamento.

Art. 10 - Principi

1. Negli atti destinati alla pubblicazione o divulgazione, i dati che permettono di identificare gli interessati sono riportati solo quando è necessario ed è previsto da una norma di legge, rispettando il principio di proporzionalità ed indispensabilità, mediante la verifica che tale pubblicazione a fini di trasparenza concerne solo dati pertinenti e non eccedenti rispetto alle finalità perseguite.

2. I sistemi informativi ed i programmi informatici devono essere configurati per ridurre al minimo l'utilizzazione di dati personali e devono prevedere la possibilità di estratti degli atti con l'esclusione dei dati personali in essi contenuti.

Art. 11 - Attività amministrativa

1. L'attività tecnico-amministrativa della SRR si svolge, principalmente, con l'emissione, la elaborazione, la riproduzione e la trasmissione di dati, compresi i procedimenti per la emanazione di provvedimenti, mediante sistemi informatici o telematici.

2. Per l'attività informatica di cui al comma precedente sono rigorosamente rispettate le norme di cui al **Codice dell'amministrazione digitale di cui al decreto legislativo 7 marzo 2005, n. 82, e sue successive modificazioni ed integrazioni, ove direttamente compatibili.**

3. La sicurezza dei dati personali è assicurata anche mediante adeguate soluzioni tecniche connesse all'utilizzo della firma digitale, chiavi biometriche o altre soluzioni tecniche.

Art. 12 - Fascicolo personale dipendenti e amministratori

1. I dati sullo stato di salute dei dipendenti e degli amministratori devono essere conservati separatamente rispetto alle altre informazioni personali. Il fascicolo, che raccoglie tutti gli atti relativi alla loro nomina/assunzione, al percorso professionale e ai fatti più significativi che li riguardano, possono mantenere la loro unitarietà, adottando accorgimenti che impediscano un accesso indiscriminato, quali l'utilizzo di sezioni o fascicoli dedicati alla custodia di eventuali dati particolari, da conservare chiusi o con modalità che riducano la possibilità di una indistinta consultazione nel corso delle ordinarie attività amministrative.

Art. 13 - Sicurezza dei dati – Misure di sicurezza – Verifiche e controlli

1. Tutta l'attività di gestione è finalizzata a:

a) ridurre al minimo il rischio di distruzione o perdita, anche accidentale, dei dati memorizzati;

b) evitare l'accesso, non autorizzato, alle banche dati, alla rete e, in generale, ai servizi informatici della SRR;

c) **prevenire trattamenti dei dati non conformi alla legge o ai regolamenti e/o la cessione o la distribuzione dei dati in caso di cessazione del trattamento.**

2. I responsabili del trattamento e delle banche dati garantiscono, anche in relazione alle conoscenze acquisite in base al progresso tecnologico, l'adozione e lo sviluppo di misure di sicurezza adeguate come: ***la pseudonimizzazione; la minimizzazione; la cifratura dei dati personali; la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico; una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento***.

3. Nella gestione dei dati personali con il sistema informatizzato dovrà essere assicurato il puntuale e scrupoloso rispetto di tutte le norme vigenti.

4. Gli stessi responsabili delle banche dati si attiveranno periodicamente con controlli, anche a campione, al fine di garantire la sicurezza delle banche dati e la esattezza e completezza dei dati inseriti.

5. Costituiscono misure tecniche ed organizzative che possono essere adottate dall'unità organizzativa cui è preposto ciascun referente/autorizzato:

- **sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; altro);**
- **misure antincendio; sistemi di rilevazione di intrusione; sistemi di sorveglianza; sistemi di protezione con videosorveglianza; registrazione accessi; porte, armadi e contenitori dotati di serrature e ignifughi; sistemi di copiatura e conservazione di archivi elettronici; altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico**.

6. Ogni ulteriore misura idonea a tutela delle banche dati personali informatiche o cartacee andrà adottata secondo un principio di proporzionalità tra le risorse disponibili e i diritti da tutelare.

Art. 14 – Trattamento e accesso ai dati particolari e giudiziari

1. Per l'accesso ai dati in rubrica, con apposito atto a firma del Presidente del CdA, sono rilasciate specifiche e formali autorizzazioni a più livelli, singole o a gruppi di lavoro, per il trattamento dei dati e la loro manutenzione. Di norma, le autorizzazioni di cui al precedente periodo sono rilasciate, con un livello di autorizzazione superiore rispetto a quello concesso nei confronti dei

semplici Autorizzati, anche ai soggetti di cui all'art. 4, comma 5, lett. b) del presente Regolamento, in quanto Designati al trattamento e Responsabili delle unità organizzative in cui si articola la struttura organizzativa dell'ente (Capi Servizio), i quali ricoprono un ruolo gestionale e di responsabilità all'interno dell'Ente, essendo preposti al sovraintendimento e al coordinamento del trattamento dei dati contenuti nelle banche dati esistenti nei Settori e negli Uffici di loro competenza, nonché alla funzione di raccordo tra la struttura di propria afferenza e l'Area funzionale di loro rispettiva appartenenza.

2. L'autorizzazione è limitata ai soli dati la cui conoscenza è necessaria e sufficiente per lo svolgimento delle operazioni assegnate agli autorizzati.

3. In attuazione del Regolamento UE 2016/679 le tabelle, raccolte nell'**ALLEGATO 1** che formano parte integrante del presente regolamento, identificano i tipi di dati particolari e giudiziari per cui è consentito il relativo trattamento, nonché le operazioni eseguibili in riferimento alle specifiche finalità di rilevante interesse pubblico perseguito.

4. I dati particolari e giudiziari individuati dal presente regolamento sono trattati previa verifica della loro pertinenza, completezza ed indispensabilità rispetto alle finalità perseguite nei singoli casi, specie nel caso in cui la raccolta non avvenga presso l'interessato.

5. I dati particolari o giudiziari non indispensabili, dei quali la SRR, nell'espletamento della propria attività istituzionale, venga incidentalmente a conoscenza ad opera dell'interessato - e comunque, non a richiesta della SRR medesima - non sono utilizzati in alcun modo, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene.

Art. 15 – Registro delle attività di trattamento 1. Il Registro delle attività di trattamento svolte dal Titolare del trattamento reca almeno le seguenti informazioni:

a) **il nome ed i dati di contatto dell'ente, del Presidente pro-tempore in carica e/o del suo Delegato ai sensi del precedente art. 2, eventualmente del Contitolare del trattamento e del DPO;**

b) **le finalità del trattamento;**

c) **la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;**

d) **le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;**

e) **l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;**

f) **ove stabiliti, i termini ultimi previsti per la conservazione e la cancellazione delle diverse categorie di dati;**

g) **il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento.**

2. Il Registro è tenuto dal Titolare ovvero dal soggetto dallo stesso delegato, presso gli uffici della struttura organizzativa della SRR, sia in forma elettronica che cartacea, secondo quanto previsto dal Regolamento UE; nello stesso possono essere inserite ulteriori informazioni tenuto conto delle dimensioni organizzative dell'ente.

Art. 16 - Diritti dell'interessato

1. I soggetti, i cui dati sono contenuti in una banca dati della SRR, hanno il diritto di ottenere, senza indugio:

a) **la conferma dell'esistenza o meno di trattamenti di dati che li riguardano, anche se non ancora registrati, e la comunicazione in forma intelligibile dei medesimi dati e della loro origine, nonché della logica e delle finalità del trattamento;**

b) **la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge;**

c) **l'aggiornamento, la rettificazione, ovvero, qualora vi abbiano interesse, l'integrazione dei dati;**

d) **l'attestazione che le operazioni di cui ai successivi commi 2 e 3 sono state portate a conoscenza dei terzi;**

2. L'interessato ha, inoltre, il diritto di opporsi, per motivi legittimi, al trattamento dei dati che lo riguardano, ancorché pertinenti allo scopo della raccolta.

3. L'interessato può esercitare tali diritti con una formale richiesta al Titolare del Trattamento. 4. L'interessato può conferire - per iscritto, delega o procura - tali diritti a persone fisiche o ad associazioni di categoria.

Art. 17 – Valutazione d'impatto sulla protezione dei dati

1. Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare, prima di effettuare il trattamento, deve attuare una valutazione dell'impatto del medesimo trattamento **(DPIA)** ai sensi dell'art. 35 del Regolamento UE, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento. La DPIA è una procedura che permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi.

2. Ai fini della decisione di effettuare o meno la DPIA si tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione come redatti e pubblicati dal Garante Privacy ai sensi dell'at. 35 del Regolamento UE.

3. La DPIA è effettuata in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche. Fermo restando quanto indicato dall'art. 35, p. 3, del Regolamento UE, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono i seguenti:

a) **trattamenti valutativi o di scoring, compresa la profilazione e attività predittive, concernenti aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato;**

b) **decisioni automatizzate che producono significativi effetti giuridici o di analoga natura, ossia trattamenti finalizzati ad assumere decisioni su interessati che producano effetti giuridici sulla persona fisica ovvero che incidono in modo analogo significativamente su dette persone fisiche;**

c) **monitoraggio sistematico, ossia trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di un'area accessibile al pubblico;**

d) **trattamenti di dati particolari o dati di natura estremamente personale, ossia le categorie particolari di dati personali di cui all'art. 9, Regolamento UE;**

e) **trattamenti di dati su larga scala, tenendo conto: del numero di numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; durata o persistenza dell'attività di trattamento; ambito geografico dell'attività di trattamento;**

f) **combinazione o raffronto di insiemi di dati, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;**

g) **dati relativi a interessati vulnerabili, ossia ogni interessato particolarmente vulnerabile e meritevole di specifica tutela per il quale si possa identificare una situazione di disequilibrio nel rapporto con il Titolare del trattamento, come i dipendenti dell'Ente, soggetti con patologie psichiatriche, richiedenti asilo, pazienti, anziani e minori;**

h) **utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative; i) tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.**

S.R.R. Trapani Provincia Sud
Società Consortile per azioni
Corso Vittorio Emanuele n°168/C
91028 Partanna TP
C.F. | P.I. 02485430819
Tel. (+39) 0924-203285
srrtrapanisud@pec.it
info@srrtrapaniprovinciasud.it
Sito internet: www.srrtrapaniprovinciasud.it

Nel caso in cui un trattamento soddisfi almeno due dei criteri sopra indicati occorre, in via generale, condurre una DPIA, salvo che il Titolare ritenga motivatamente che non può presentare un rischio elevato; il Titolare può motivatamente ritenere che per un trattamento che soddisfa solo uno dei criteri di cui sopra occorra comunque la conduzione di una DPIA.

4. Il Titolare garantisce l'effettuazione della DPIA ed è responsabile della stessa. Il Titolare può affidare la conduzione materiale della DPIA ad un altro soggetto, interno o esterno alla SRR. Il Titolare deve consultarsi con il DPO anche per assumere la decisione di effettuare o meno la DPIA; tale consultazione e le conseguenti decisioni assunte dal Titolare devono essere documentate nell'ambito della DPIA. Il DPO monitora lo svolgimento della DPIA. Il Responsabile del trattamento deve assistere il Titolare nella conduzione della DPIA fornendo ogni informazione necessaria. **Il responsabile della sicurezza dei sistemi informativi, se nominato, e/o l'ufficio competente per detti sistemi**, forniscono supporto al Titolare per lo svolgimento della DPIA.

5. Il DPO può proporre lo svolgimento di una DPIA in rapporto a uno specifico trattamento, collaborando al fine di mettere a punto la relativa metodologia, definire la qualità del processo di valutazione del rischio e l'accettabilità o meno del livello di rischio residuale.

Il responsabile della sicurezza dei sistemi informativi, se nominato, e/o l'ufficio competente per detti sistemi, possono proporre di condurre una DPIA in relazione a uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.

6. La DPIA non è necessaria nei casi seguenti:

➢ **se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35, p. 1, Regolamento UE;**

➢ **se la natura, l'ambito, il contesto e le finalità del trattamento sono simili a quelli di un trattamento per il quale è già stata condotta una DPIA. In questo caso si possono utilizzare i risultati della DPIA svolta per l'analogo trattamento;**

➢ **se il trattamento è stato sottoposto a verifica da parte del Garante Privacy in condizioni specifiche che non hanno subito modifiche;**

➢ **se un trattamento trova la propria base legale nella vigente legislazione che disciplina lo specifico trattamento, ed è già stata condotta una DPIA all'atto della definizione della base giuridica suddetta**.

Non è necessario condurre una DPIA per quei trattamenti che siano già stati oggetto di verifica preliminare da parte del Garante della Privacy o da un DPO e che proseguano con le stesse modalità oggetto di tale verifica.

7. La DPIA è condotta prima di dar luogo al trattamento, attraverso i seguenti processi:

a) **descrizione sistematica del contesto, dei trattamenti previsti, delle finalità del trattamento e tenendo conto dell'osservanza di codici di condotta approvati. Sono altresì indicati: i dati personali oggetto del trattamento, i destinatari e il periodo previsto di conservazione dei dati stessi; una descrizione funzionale del trattamento; gli strumenti coinvolti nel trattamento dei dati personali** (hardware, software, reti, persone, supporti cartacei o canali di trasmissione cartacei);

b) **valutazione della necessità e proporzionalità dei trattamenti, sulla base:**

- delle finalità specifiche, esplicite e legittime;
- della liceità del trattamento;
- dei dati adeguati, pertinenti e limitati a quanto necessario;
- del periodo limitato di conservazione;
- delle informazioni fornite agli interessati;
- del diritto di accesso e portabilità dei dati;
- del diritto di rettifica e cancellazione, di opposizione e limitazione del trattamento;
- dei rapporti con i responsabili del trattamento;
- delle garanzie per i trasferimenti internazionali di dati;
- consultazione preventiva del Garante privacy;

d) **valutazione dei rischi per i diritti e le libertà degli interessati, valutando la particolare probabilità e gravità dei rischi rilevati. Sono determinati l'origine, la natura, la particolarità e la gravità dei rischi o, in modo più specifico, di ogni singolo rischio (accesso illegittimo, modifiche indesiderate, indisponibilità dei dati) dal punto di vista degli interessati;**

e) **individuazione delle misure previste per affrontare ed attenuare i rischi, assicurare la protezione dei dati personali e dimostrare la conformità del trattamento con il Regolamento UE, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.** 8. Il Titolare può raccogliere le opinioni degli interessati o dei loro rappresentanti, se gli stessi possono essere preventivamente individuati. La mancata consultazione è specificatamente motivata, così come la decisione assunta in senso difforme dall'opinione degli interessati.

9. Il Titolare deve consultare il Garante Privacy prima di procedere al trattamento se le risultanze della DPIA condotta indicano l'esistenza di un rischio residuale elevato. Il Titolare consulta il

Garante Privacy anche nei casi in cui la vigente legislazione stabilisce l'obbligo di consultare e/o ottenere la previa autorizzazione della medesima autorità, per trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale ed alla sanità pubblica.

Art. 18 – Entrata in vigore e normativa applicabile

1. Il presente regolamento entra in vigore il giorno successivo a quello di sua avvenuta pubblicazione sul profilo informatico istituzionale della SRR, di cui al seguente art. 21.

2. Per quanto non previsto nel presente regolamento trovano applicazione:

a) **le direttive ed i regolamenti comunitari, le leggi nazionali e regionali in materia vigenti e all'uopo applicabili;**

b) **lo statuto della SRR;**

c) **il Regolamento interno sull'organizzazione generale degli uffici e dei servizi;**

d) **Eventuali procedure operative, circolari di raccomandazione e/o istruzioni et similia.**

Art. 19 - Rinvio dinamico

1. Le norme del presente regolamento si intendono modificate per effetto di sopravvenute norme vincolanti euro-unitarie per la parte direttamente applicabile, statali e regionali.

2. In tali casi, in attesa della formale modificazione del presente regolamento, si applica la normativa sovraordinata.

Art. 20 - Norme abrogate

1. Con l'entrata in vigore del presente regolamento sono abrogate tutte le eventuali norme regolamentari con esso contrastanti.

Art. 21 - Pubblicità del regolamento

1. Copia del presente regolamento, unitamente ai propri allegati (***All. 1 - "Tipi di dati particolari e giudiziari per cui è consentito il relativo trattamento" – All. 2 – Organigramma Privacy***), che costituiscono parte integrante e sostanziale dello stesso, è pubblicato nell'apposita sezione di *"Amministrazione trasparente"* del sito internet istituzionale

S.R.R. Trapani Provincia Sud Soc. Consortile s.p.a.