Regolamento Attuativo GDPR di Siena Parcheggi Spa

Approvato nella seduta del Consiglio di Amministrazione in data 7 giugno 2019

Introduzione

Il presente Regolamento attuativo del Nuovo Regolamento EU GDPR 679/2016 (da qui in avanti "RGPD") è stato elaborato alla luce dell'introduzione da parte del RGPD del principio di responsabilizzazione, cd. *accountability*, a cui deve integralmente conformarsi il trattamento dei dati personali a partire dal 25 maggio 2018.

Il considerando (da qui in avanti "c.") 74 RGPD determina il contenuto del principio di responsabilizzazione. Questo combina due aspetti: l'adozione da parte del Titolare del trattamento di misure adeguate ed efficaci ai sensi dell'art. 24 co. 1 RGPD e la capacità di dimostrare la conformità delle attività di trattamento alle disposizioni del RGPD.
Il Titolare del trattamento ha l'obbligo di attuare misure e procedure interne al fine di rendere effettivi i principi di protezione dei dati, assicurandone l'efficacia e, qualora l'autorità di protezione dei dati ne faccia richiesta, di dimostrare la concreta attuazione di tali principi.

L'*accountability* richiede l'aderenza ai principi generali del trattamento di cui all'art. 5 co. 1 RGPD attraverso l'adozione delle misure adeguate ai sensi dell'art. 24 co. 1 RGPD. Per 'adeguate' si intendono, alla luce del combinato disposto tra il c.74 e l'art. 24 co. 1 RGPD, le misure poste in essere in conseguenza di una valutazione ex ante - ossia compiuta dal titolare prima dell'effettuazione del trattamento - della natura, del campo di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche. E' necessaria, dunque, una valutazione concreta, da effettuarsi caso per caso.
Ai sensi dell'art. 24 co. 1 RGPD, il principio di responsabilizzazione richiede anche una verifica ex post dell'efficacia delle misure. Il titolare non solo deve adottare delle misure appropriate, ma deve anche valutarne l'efficacia attraverso degli appositi strumenti di valutazione.
Infine, il principio di *accountability* si manifesta con la necessità, per il titolare, di essere in grado di dimostrare, all'autorità che ne faccia richiesta, se e come ha attuato le misure che garantiscono un trattamento conforme ai principi del RGPD.

La nuova disciplina, non prevedendo più una serie di 'misure minime' da adottare - quali quelle contenute nell'allegato B al Codice Privacy – richiede di individuare, di volta in volta, le misure adeguate alla luce degli elementi sopra indicati. L'introduzione del concetto di *accountability* lascia maggiore discrezionalità al titolare del trattamento nel decidere attraverso quali modalità tutelare i dati; a tale libertà si accompagna l'onere, in capo a tale soggetto, di dimostrare perché ha preso una determinata decisione, oltre che di documentare le scelte effettuate. Spetta al titolare individuare e adattare al caso specifico le misure necessarie per garantire la

conformità effettiva dei trattamenti alle norme del regolamento e quindi la garanzia della tutela e protezione reale dei dati personali.

In sostanza, vi sono due livelli di responsabilità. Il primo è costituito da un obbligo di base vincolante per tutti i titolari/responsabili e integrato da disposizioni specifiche, le quali stabiliscono i requisiti in presenza dei quali sussiste il vincolo di adozione di determinate misure; tale obbligo implica l'attuazione di misure adeguate ed efficaci e la conservazione delle relative prove. Il secondo riguarda le misure volontarie che perfezionano il principio di responsabilizzazione, superando le norme imperative minime, e che rappresentano un'ulteriore garanzia del rispetto dei principi fondamentali di protezione dei dati e riducono i margini di rischio del trattamento.

Il presente documento ha per oggetto l'adozione delle misure procedimentali e delle regole necessarie per dare attuazione al Regolamento europeo (General Data Protection Regulation del 27 aprile 2016 n. 679, di seguito indicato con "RGPD", Regolamento Generale Protezione Dati), relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione di tali dati.

Art. 1

Titolare del trattamento dei dati personali

1. **Siena Parcheggi Spa** nella persona del proprio legale rappresentante in carica, è il Titolare del trattamento dei dati personali (di seguito, per semplicità, "trattamento") raccolti o meno in banche dati, automatizzate o cartacee (di seguito indicato con "Titolare").
2. Il Titolare determina le finalità e i mezzi del trattamento di dati personali e decide sul profilo della sicurezza.
3. Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 RGPD: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.
4. Il Titolare mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento dei dati personali è effettuato in modo conforme al RGPD. Il Titolare deve verificare e aggiornare dette misure qualora necessario.
5. Le misure sono definite dal Titolare 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, così come descritti dagli articoli da 15 a 22 RGPD, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio.
6. Ai sensi dell'art. 35 RGPD, nel caso in cui un tipo di trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, in particolare se prevede l'uso di nuove tecnologie, il Titolare deve effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito "DPIA"). Qualora la DPIA indichi che il trattamento

presenti un rischio elevato in assenza di misure adottate dal Titolare per attenuarne il rischio, questi, prima di procedere al trattamento, consulta l'autorità di controllo.

7. Il Titolare sceglie consapevolmente i soggetti che ricoprono i ruoli subalterni e li istruisce. Provvede a:

a) designare i Responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del RGPD e garantisca la tutela dei diritti dell'interessato;

b) nominare, nei casi previsti dal RGPD, il Responsabile della protezione dei dati, scegliendolo tra i soggetti che hanno esperienza e professionalità giuridica, anche sotto il profilo applicativo;

c) fornire istruzioni adeguate al personale che tratta i dati.

8. Nel caso di violazione dei dati personali deve porre in essere contromisure effettive e tempestive e procedere alla notificazione al Garante ai sensi dell'art. 33 RGPD e, nei casi previsti, alla comunicazione all'interessato ai sensi dell'art. 34 RGPD.

9. Il Titolare adotta misura appropriate per fornire all'interessato:

a) le informazioni indicate dall'art. 13 RGPD, qualora i dati personali siano raccolti presso lo stesso interessato;

b) le informazioni indicate dall'art. 14 RGPD, qualora i dati personali non siano stati ottenuti presso lo stesso interessato.

Successivamente, si dota di idonea organizzazione per riscontrare tempestivamente le istanze dell'interessato e per permettere l'esercizio dei diritti riconosciuti così come esposto all'art. 1.5 del presente Regolamento.

10. Allorché due o più titolari determinano congiuntamente, mediante accordo, le finalità ed i mezzi del trattamento, si realizza la contitolarità di cui all'art. 26 RGPD. L'accordo definisce le responsabilità di ciascuno in merito all'osservanza degli obblighi in tema di privacy, con particolare riferimento all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli artt. 13 e 14 del RGPD, fermo restando eventualmente quanto stabilito dalla normativa specificatamente applicabile; l'accordo può individuare un punto di contatto comune per gli interessati.

12. Il Titolare non intende al momento aderire ai codici di condotta elaborati da eventuali associazioni e dagli organismi di categoria rappresentativi, ovvero a meccanismi di certificazione della protezione dei dati approvati, per contribuire alla corretta applicazione del RGPD e per dimostrarne il concreto rispetto da parte del Titolare e dei Responsabili del trattamento.

Art. 2

Finalità del trattamento

1. I trattamenti sono compiuti da **Siena Parcheggi Spa** per le seguenti finalità:

- Consentire l'erogazione dei Servizi richiesti, inclusa la raccolta, la conservazione e la elaborazione dei dati ai fini dell'instaurazione e della successiva gestione

operativa, tecnica ed amministrativa del rapporto connesso all'erogazione dei Servizi e l'effettuazione di comunicazioni relative allo svolgimento del rapporto instaurato;

- rispondere a richieste di assistenza o di informazioni, ricevute via e-mail, telefono o chat attraverso l'apposito form del sito internet;
- assolvere obblighi di legge, contabili e fiscali;
- eventualmente, elaborare studi, ricerche, statistiche di mercato; inviare materiale pubblicitario, informativo, informazioni commerciali o sondaggi indiretti per migliorare il servizio via e-mail e/o attraverso l'uso del telefono.

per specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento.

2. Il trattamento dei dati personali per finalità diverse da quelle per le quali i dati personali sono stati inizialmente raccolti è consentito solo se compatibile con le finalità per le quali i dati personali sono stati inizialmente raccolti. In tal caso non è richiesta alcuna base giuridica separata oltre a quella che ha consentito la raccolta dei dati personali.
Per accertare la compatibilità tra la finalità di un ulteriore trattamento e quella per la quale i dati sono stati inizialmente raccolti, spetta al Titolare valutare:
a) ogni nesso tra le finalità originarie e quelle successive, il contesto in cui i dati personali sono stati raccolti e, in particolare, le ragionevoli aspettative dell'interessato in base alla sua relazione con il titolare del trattamento con riguardo al loro ulteriore utilizzo;
b) la natura dei dati personali;
c) le conseguenze dell'ulteriore trattamento previsto per gli interessati;
d) l'esistenza di garanzie adeguate sia nel trattamento originario sia nell'ulteriore trattamento previsto.

ART. 3

Principi applicati al trattamento

1. Secondo quanto disposto dall'art. 5. Co. 1 lett. a) e dal c. 39 RGPD, il trattamento dei dati personali avviene in modo lecito e corretto.
Il trattamento dei dati personali avviene soltanto su espresso consenso dell'interessato o, in alternativa, nel caso in cui tale trattamento trovi fondamento normativo nel RGPD o in altra fonte comunitaria o nazionale (c.40).
Gli interessati sono informati circa la raccolta, l'utilizzo, la consultazione e le ulteriori tipologie di trattamenti effettuate, precisando in che misura essi sono e saranno trattati. Le comunicazioni, alla luce del principio di trasparenza, avvengono attraverso un linguaggio semplice e chiaro (c.39).

2. Secondo quanto disposto dall'art. 5 co. 1 lett. b) RGPD, i dati personali sono raccolti per finalità determinate, esplicite e legittime.

Il trattamento successivo dei dati raccolti non potrà avvenire in modo incompatibile con le finalità originarie; per questo è previsto che il titolare effettuerà una valutazione di compatibilità tra le finalità iniziali e quelle successive.

Tale divieto non opera nei seguenti casi:

a) il trattamento ulteriore dei dati personali è necessario per finalità di archiviazione nel pubblico interesse o per finalità statistiche o di ricerca scientifica o storica;

b) Il trattamento ha fondamento in una norma di diritto comunitario o nazionale che costituisce una misura necessaria e proporzionata in una società democratica per salvaguardare obiettivi di interesse pubblico generale;

c) Il titolare abbia degli interessi legittimi che prevalgono su quelli dell'interessato.

3. Secondo quanto disposto dall'art. 5 co. 1 lett. c) RGPD, sono raccolti soltanto i dati personali funzionali al perseguimento delle finalità predeterminate (*privacy by default*).

4. Secondo quanto disposto dall' Art. 5 co. 1 lett. d) RGPD il Titolare del trattamento tratta i dati personali esatti, aggiornandoli e organizzando la sua struttura in modo da garantire l'accuratezza delle informazioni personali.

In forza dell'art. 16 RGPD l'interessato ha il diritto di rettifica nel caso in cui i suoi dati personali trattati siano inesatti, compresi anche i dati non aggiornati. Qualora ciò non sia possibile o non venga effettuato l'aggiornamento, gli stessi saranno cancellati.

In forza dell'art. 18 RGPD l'interessato ha il diritto di contestare il trattamento dei dati personali.

5. Secondo quanto disposto dall'art. 5 co. 1 lett. e) RGPD i dati sono conservati in modo da permettere l'identificazione dell'interessato solo per il tempo necessario a conseguire le finalità del trattamento.

Nei casi che derogano a tale principio ai sensi dell'art. 23 RGPD, sono adottate adeguate misure tecniche e organizzative richieste dal RGPD volte a proteggere i diritti e le libertà dell'interessato.

6. Secondo quanto disposto dall'art. 5.1.f) ai dati personali raccolti viene garantita l'adeguata sicurezza sia preventiva che successiva.

ART. 4

Responsabile del trattamento

1. Il Titolare può avvalersi, per il trattamento di dati, anche di quelli descritti dagli artt. 9 e 10 RGPD, di soggetti pubblici o privati che, in qualità di Responsabili del trattamento, forniscano le garanzie sufficienti in termini di conoscenza specialistica, esperienza, capacità ed affidabilità, per mettere in atto le misure tecniche ed organizzative adeguate ai sensi dell'art. 28 RGPD, stipulando atti giuridici in forma scritta, che specificano la finalità perseguita, la tipologia dei dati, la durata del trattamento, gli obblighi e i diritti del responsabile del trattamento e le

modalità di trattamento.
2. Gli atti che disciplinano il rapporto tra il Titolare ed il Responsabile del trattamento devono contenere quanto previsto dall'art. 28 co. 3 RGPD. Tali atti possono anche basarsi su clausole contrattuali tipo adottate dal Garante per la protezione dei dati personali oppure dalla Commissione europea.
4. L'atto giuridico con cui il Titolare effettua la nomina deve prevedere quanto previsto dall'art. 28 RGPD; nello specifico deve prevedere che il Responsabile del trattamento:
a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, secondo quanto specificato dall'art. 28 co. 3 lett. a) RGPD;
b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
c) adotti tutte le misure richieste ai sensi dell'art. 32 RGPD;
d) rispetti le condizioni di cui agli artt. 28 co. 2 e 28 co. 4 per ricorrere a un altro responsabile del trattamento;
e) tenendo conto della natura del trattamento, assista il Titolare con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del Titolare di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III del RGPD;
f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 RGPD, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
g) su scelta del Titolare, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, così come descritto dall'art. 28 co. 3 lett. g) RGPD;
h) metta a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'art. 28 RGPD e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal Titolare o da un altro soggetto da Questi incaricato.
5. E' consentita la nomina di sub-responsabili del trattamento da parte di ciascun Responsabile del trattamento per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano il Titolare ed il Responsabile primario; le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del Responsabile attenendosi alle istruzioni loro impartite per iscritto che individuano specificatamente l'ambito del trattamento consentito.
Il Responsabile risponde, anche dinanzi al Titolare, dell'operato del sub-responsabile anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso non gli è in alcun modo imputabile e che ha vigilato in modo adeguato sull'operato del sub-responsabile.
6. Il Responsabile del trattamento garantisce che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali sia in possesso di apposita formazione ed istruzione e si sia

impegnato alla riservatezza od abbia un adeguato obbligo legale di riservatezza.
7. Il Responsabile del trattamento dei dati 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 provvede:
a) alla tenuta del registro delle categorie di attività di trattamento svolte per conto del Titolare;
b) all'adozione di idonee misure tecniche e organizzative adeguate per garantire la sicurezza dei trattamenti;
c) alla sensibilizzazione ed alla formazione del personale che partecipa ai trattamenti ed alle connesse attività di controllo;
d) alla designazione del Responsabile per la Protezione dei Dati (RPD), se a ciò demandato dal Titolare;
e) ad assistere il Titolare nella conduzione DPIA fornendo allo stesso ogni informazione di cui è in possesso;
f) ad informare il Titolare, senza ingiustificato ritardo, della conoscenza di casi di violazione dei dati personali (cd. "data breach"), per la successiva notifica della violazione al Garante Privacy, a meno che il Titolare stesso ritenga improbabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati.
8. Il Titolare del Trattamento **Siena Parcheggi Spa**, nella persona del proprio legale rappresentante in carica, individua, previa apposita e separata nomina secondo quanto indicato dall'art. 4 del presente documento, quali Responsabili del Trattamento ai sensi dell'art. 28 RGPD, i soggetti elencati all'interno del documento allegato.

ART. 5

Responsabile della protezione dei dati

1. La Società **Siena Parcheggi Spa,** nella persona del proprio legale rappresentante in carica è a conoscenza che, ai sensi dell'art. 37 RGPD:
a) Il titolare del trattamento e il responsabile del trattamento devono designare sistematicamente un responsabile della protezione dei dati, obbligatoriamente, nei casi previsti dall'art. 37 co. 1 RGPD e 37 co. 4 RGPD e facoltativamente nel caso previsto dall'art. 37 co. 4 RGPD;
b) Le modalità di designazione sono descritte dall'art. 37 co. 2 e 37 co. 3 RGPD;
c) Le qualità soggettive del responsabile della protezione dei dati sono previste dall'art. 37 co. 5 e 37 co. 6 RGPD;
d) Il titolare del trattamento o il responsabile del trattamento ha l'obbligo di pubblicazione di cui all'art. 37 co. 7 RGPD.
2. La Società **Siena Parcheggi Spa**, osserva che:
a) E' una società in *house* del Comune di Siena;
b) Svolge, in qualità di soggetto incaricato di pubblico servizio, monitoraggio regolare e sistematico degli interessati su larga scala quale attività principale e comunque un'attività di

vigilanza che rientra nei casi di Nomina come previsto dalle linee guida;
c) Le attività principali riguardano dati sensibili di cui all'art. 9 RGPD o giudiziari di cui all'art. 10 RGPD su larga scala;
d) Intende nominare un responsabile della protezione dati.
3. La Società **Siena Parcheggi Spa,** dichiara di nominare un Responsabile della protezione dati. Vedi atto di nomina allegato.

ART. 6

Registri delle attività di trattamento

1. La Società **Siena Parcheggi Spa**, nella persona del proprio legale rappresentante in carica è a conoscenza che, ai sensi dell'art. 30 RGPD:
a) ogni titolare del trattamento e, ove applicabile, il suo rappresentante in carica, devono tenere un registro delle attività del trattamento svolte sotto la propria responsabilità, contenente le informazioni previste dall'art. 30.1 RGPD;
b) ogni responsabile del trattamento e, ove applicabile, il suo rappresentante in carica, tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente le informazioni previste dall'art. 30 co. 2 RGPD;
c) i registri devono possedere i requisiti di forma previsti dall'art. 30 co. 3 RGPD;
d) il registro deve essere messo a disposizione dell'autorità di controllo ai sensi dell'art. 30 co. 4 RGPD;
e) l'30 co. 5 RGPD prevede i soggetti per i quali non si applicano gli obblighi di cui ai paragrafi 1 e 2;
2. La Società **Siena Parcheggi Spa,** osserva che:
a) l'attuale numero dei dipendenti è inferiore a 250 unità,
b) il trattamento dei dati effettuati dalla Società non presenta un rischio per i diritti e le libertà dell'interessato, non sia occasionale o includa il trattamento di dati sensibili o giudiziari.
3. La Società **Siena Parcheggi Spa** dichiara, ai sensi dall'art. 30 co. 5 RGPD, di voler lo stesso adempiere all'obbligo di creazione e mantenimento del Registro delle attività di trattamento di cui all'art. 30 RGPD come suggerito anche dalle linee guida del WP art. 29 (vedi Allegato).

ART. 7

Valutazione d'impatto sulla protezione dei dati

1. La Società **Siena Parcheggi Spa** nella persona del proprio legale rappresentante in carica è a conoscenza che, ai sensi dell'art. 35 RGPD, il titolare del trattamento ha l'obbligo di effettuare la valutazione di impatto nel caso in cui:
a) La raccolta dei dati personali avvenga attraverso l'utilizzazione di nuove tecnologie (art. 35 co. 1 RGPD);
b) Vi sia, valutati la natura, l'oggetto, il contesto e le finalità del trattamento, un rischio elevato (C.76 RGPD) per i diritti e le libertà delle persone fisiche (art. 35 co. 1 RGPD);

c) Il trattamento prevede una valutazione sistematica e globale di aspetti personali relativi alle persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche (Art. 35 co. 3 RGPD);
d) Il trattamento riguardi, su larga scala, le categorie particolari di dati personali di cui all'art. 9 co. 1. RGPD, ossia dati sensibili ovvero dati relativi a condanne penali e ai reati di cui all'art. 10 RGPD (Art. 35 co. 3 RGPD);
e) Vi sia la sorveglianza sistematica su larga scala in una zona accessibile al gruppo (Art. 35 co. 3 RGPD);
preso atto delle deroghe previste dall'art. 35 co. 10 RGPD,
2. Dichiara di effettuare la valutazione di impatto del trattamento, utilizzando a tal fine il modello allegato.

ART. 8

Sicurezza del trattamento

1. Il Titolare e ciascun Responsabile del trattamento mettono in atto misure tecniche ed organizzative per 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.
2. Le misure tecniche ed organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento ricomprendono, tra le altre:
a) la pseudonimizzazione;
b) la minimizzazione;
c) la cifratura dei dati personali;
d) la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali;
e) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;
f) una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
3. Costituiscono misure tecniche ed organizzative che possono essere adottate:
a) sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; altro);
b) 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.
4. La conformità del trattamento dei dati al RGPD in materia di protezione dei dati personali è dimostrata attraverso l'adozione delle misure di sicurezza o l'adesione a codici di condotta approvati di cui all'articolo 40 RGPD o ad un meccanismo di certificazione approvato di cui all'art. 42 RGPD.
5. Il Titolare e ciascun Responsabile del trattamento si obbligano ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali.
6. I nominativi ed i dati di contatto del Titolare, del o dei Responsabili del trattamento sono pubblicati oltre che nella sezione "privacy" del sito sono disponibili presso l'ufficio amministrativo previa richiesta.

ART. 9

Violazione dei dati personali

1. Per violazione dei dati personali (in 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 dall'azienda.
2. Il Titolare, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, provvede alla notifica della violazione al Garante Privacy. La notifica dovrà avvenire entro 72 ore e comunque senza ingiustificato ritardo. Il Responsabile del trattamento è obbligato ad informare il Titolare, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione.
3. I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 del RGPD, sono i seguenti:
- 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.
- decifratura non autorizzata della pseudonimizzazione;
- pregiudizio alla reputazione;
- perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).
4. Se il Titolare ritiene che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata è elevato, allora deve informare questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di fare comprendere loro la natura della violazione dei dati personali verificatesi.
I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la

violazione può, a titolo di esempio:
- 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 (ad esempio dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
- comportare rischi imminenti e con un'elevata probabilità di accadimento (ad esempio rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);
- impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (ad esempio utenti deboli, minori, soggetti indagati).

5. La notifica deve avere il contenuto minimo previsto dall'art. 33 RGPD, ed anche la comunicazione all'interessato deve contenere almeno le informazioni e le misure di cui al citato art. 33 RGPD. A tal proposito **Siena Parcheggi Spa** ha elaborato una procedura inserita descritta nel capitolo MOP (Modello Organizzativo Privacy) del Manuale Privacy.

6. Il Titolare deve opportunamente documentare 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 RGPD.

ART. 10

Procedure per consentire l'esercizio dei diritti di cui agli Art. 15,16,17,18,19,20 RGDP

1. Ai sensi dell'art. 15 RGPD, l'interessato ha il diritto di ottenere dal Titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle informazioni di cui all'art. 15 co. 1 RGPD. Qualora i dati personali siano trasferiti a un paese terzo ovvero ad un'organizzazione internazionale, il titolare informerà l'interessato dell'esistenza di garanzie adeguate ai sensi dell'art. 46 RGPD.

A tal fine, la Società **Siena Parcheggi Spa** utilizza la procedura descritta nel capitolo MOP (Modello Organizzativo Privacy) del Manuale Privacy.

2. Ai sensi dell'art. 16 RGPD, l'interessato ha il diritto di ottenere dal Titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo.

A tal fine, la Società **Siena Parcheggi Spa** utilizza la procedura descritta nel capitolo MOP (Modello Organizzativo Privacy) del Manuale Privacy.

3. Ai sensi dell'art. 17 RGPD, il Titolare del trattamento, qualora l'interessato ne faccia richiesta e ricorrano le condizioni di cui all'art. 17 RGPD, ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali. Il Titolare del trattamento, se ha reso pubblici i dati personali ed è obbligato a cancellarli ai sensi dell'art. 17 GDPR, adotterà le misure ragionevoli per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.

A tal fine, la Società **Siena Parcheggi Spa** utilizza la procedura descritta nel capitolo MOP (Modello Organizzativo Privacy) del Manuale Privacy.

4. Ai sensi dell'art. 18 RGPD, quando ricorre una delle ipotesi descritte nel medesimo articolo, l'interessato ha il diritto di ottenere dal Titolare del trattamento la limitazione del trattamento.

A tal fine, la Società **Siena Parcheggi Spa** utilizza la procedura descritta nel capitolo MOP (Modello Organizzativo Privacy) del Manuale Privacy.

5. Ai sensi dell'art. 19 RGPD il Titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate a norma degli artt. 16,17, 18, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il Titolare del trattamento comunica all'interessato tali destinatari, qualora l'interessato lo richieda.

A tal fine, la Società **Siena Parcheggi Spa** utilizza la procedura descritta nel capitolo MOP (Modello Organizzativo Privacy) del Manuale Privacy.

6. Ai sensi dell'art. 20 GDPR, l'interessato del trattamento ha il diritto di ricevere dal titolare i dati personali in un formato strutturato, di uso comune e leggibile da un dispositivo automatico. L'interessato ha inoltre il diritto di ottenere, se tecnicamente fattibile, la trasmissione diretta e senza impedimenti ad altro titolare da lui indicato. L'esercizio di tale diritto è a titolo gratuito, fatta salva la facoltà del Titolare di addebitare un ragionevole contributo spese ovvero di rifiutare l'istanza qualora sia manifestamente infondata o eccessiva.

A tal fine, la Società **Siena Parcheggi Spa** utilizza la procedura descritta nel capitolo MOP (Modello Organizzativo Privacy) del Manuale Privacy.

ART. 11

Programma di formazione per gli addetti e delegati

L'art. 29 del sopra citato regolamento prevede, infatti, che "il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso ai dati personali non può trattare tali dati se non è istruito in tal senso dal titolare".

Il Gruppo di lavoro ex 29 nel parere n. 3/2010 aveva individuato tra le misure comuni concernenti la responsabilità "un'adeguata formazione ed istruzione del personale in materia di protezione dei dati. Il personale in questione dovrebbe includere gli incaricati (o responsabili) del trattamento dei dati personali, ma anche dirigenti e sviluppatori in campo informatico e direttori di unità commerciali".

La centralità della formazione è confermata anche dall'art. 32 "Sicurezza del trattamento" paragrafo 4 che prevede che "il titolare del trattamento ed il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri".

La formazione costituisce, pertanto, un prerequisito per potere operare all'interno delle organizzazioni, imprese e pubbliche amministrazioni. Essa dovrebbe, alla luce dell'impianto del

Regolamento, presentare un taglio interdisciplinare (con sessioni sia informatiche sia giuridiche sia sui profili organizzativi dell'Ente o Società) e pragmatico (come si evince dal termine "istruito" previsto all'art 29 e 32 del Regolamento) e riguardare tutti i soggetti.

La formazione dovrebbe essere finalizzata ad illustrare i rischi generali e specifici dei trattamenti di dati, le misure organizzative, tecniche ed informatiche adottate, nonché le responsabilità e le sanzioni. L'obbligo formativo non deve essere in alcun modo sottovalutato da parte delle pubbliche amministrazioni e delle imprese: nel caso di mancata erogazione della formazione scatta, infatti, ai sensi dell'art. 83 par 4 del Regolamento privacy europeo, la rilevante sanzione amministrativa pecuniaria fino a 10 milioni di euro o, per le imprese, fino a 2 % del fatturato mondiale annuo dell'anno precedente se superiore.
L'adempimento degli obblighi formativi è sovente oggetto anche di accertamenti ispettivi da parte dell'Autorità Garante privacy e da parte della Guardia di Finanza.

Il Garante, in diversi casi, in sede ispettiva ha richiesto, infatti, di acquisire il programma ed il piano di formazione, le dispense, i materiali erogati, il test finale ed ha analizzato il profilo delle istruzioni agli incaricati al trattamento connesse all'accesso, alla consultazione delle banche dati, i livelli di autorizzazione e policy aziendali (ad esempio in materia di password aziendali e di videosorveglianza).

Siena Parcheggi Spa pertanto ha programmato :

- un percorso ed un piano di formazione;
- accantonato adeguate risorse in sede di approvazione di bilancio;
- previsto prove finali nel percorso formativo, e sessioni di aggiornamento alla luce delle modifiche normative, organizzative e tecniche;
- individuato un percorso formativo alternativo, in caso di mancato superamento del test finale, ed un nuovo esame di verifica;

Nella progettazione dei corsi di formazione, **Siena Parcheggi Spa** ha esaminato e individuato : i fabbisogni formativi, la struttura dell'impresa, i profili organizzativi, il target, i prerequisiti, le finalità generali e specifiche di ciascuna sessione formativa nonché le relative modalità di erogazione (in aula o a distanza) ed i precedenti corsi predisposti in materia. Ha individuato nelle figure apicali, negli amministratori di sistema, nei nuovi assunti ed infine nelle persone autorizzate al trattamento le risorse primarie da sensibilizzare e rendere consapevoli.
Queste ultime, corrispondono agli ex incaricati del codice privacy e sono, sostanzialmente, tutti coloro che trattano dati personali.

ART. 11

Rinvio

Per tutto quanto non espressamente disciplinato con le presenti disposizioni, si applicano le disposizioni del RGPD e tutte le sue norme attuative vigenti.

ART. 12

Revisione

Il presente documento ed i relativi allegati saranno riesaminati e adeguati, se necessario, in caso di adeguamento normativo.

ALLEGATI:

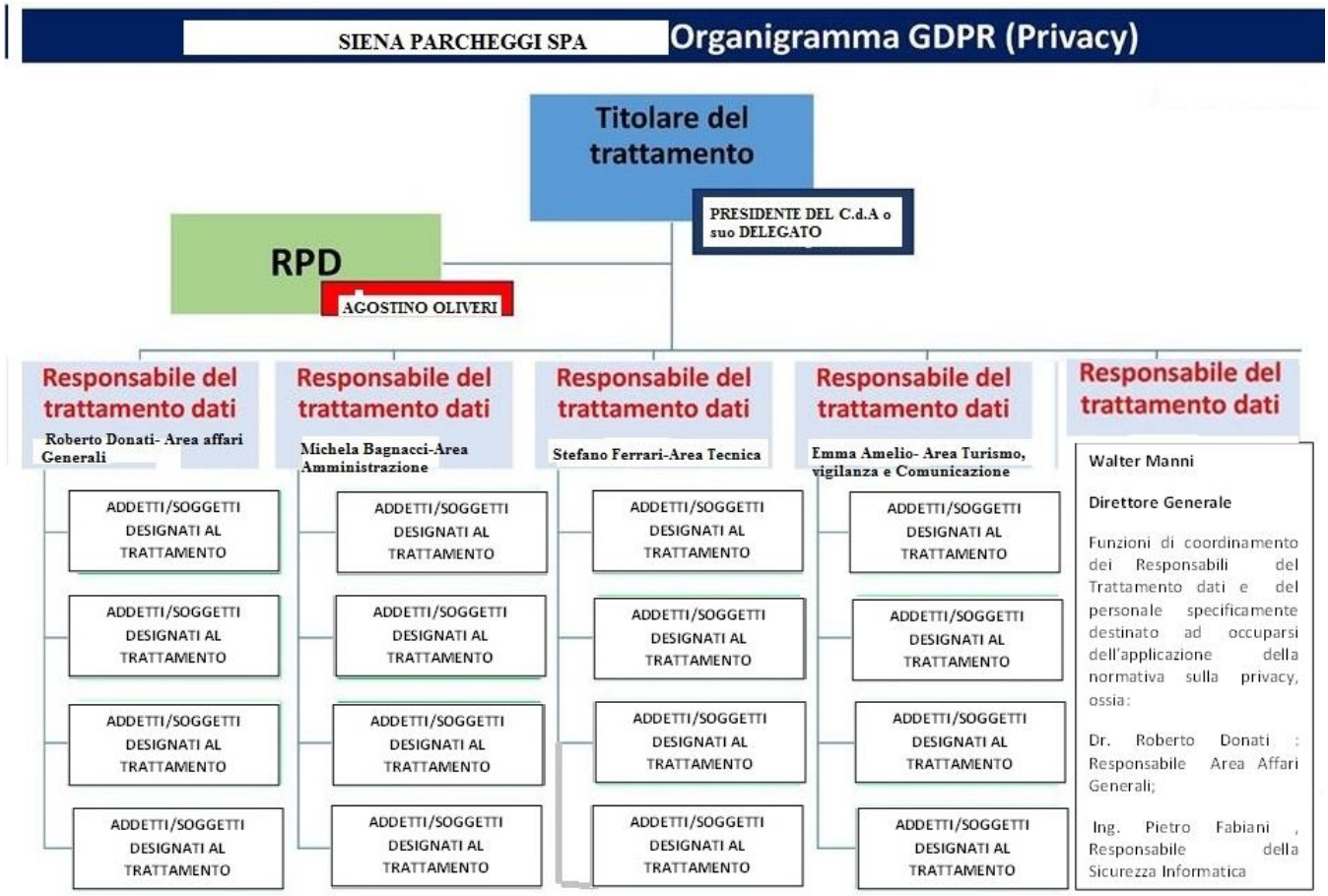
1) Organigramma

Siena,

Firma e Timbro
Titolare del Trattamento

_____

ALLEGATO 1



Il Presidente

Massimo Castagnini

Il Direttore Generale

Walter Manni