

Comune di Piscina

D.Lgs. 30/06/2003 n°196

Documento Programmatico Sulla Sicurezza

Aggiornato al 11/9/2015

Sommario

Elenco dei trattamenti dei dati personali	3
Distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati	5
Analisi dei rischi e misure minime di sicurezza da adottare	7
Banca dati Anagrafe – Elettorale - Protocollo	8
Banca dati Stato Civile	9
Banca dati Tributaria	10
Banca dati Ragioneria	11
Banca dati Rapporti lavorativi	12
Banca dati Pratiche edilizie	13
Banca dati Polizia Municipale	14
Banca dati Archivio corrente - storico	15
Banca dati Biblioteca	16
Banca dati Utenti servizi comunali Segreteria	17
Banca dati Videosorveglianza	18
Descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento	19
Descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare	20
Criteri da adottare per la cifratura o per la separazione dei dati personali idonei a rivelare lo stato di salute e la vita sessuale dagli altri dati personali dell'interessato	21

Elenco dei trattamenti dei dati personali

Nella Tabella 1 sono elencati i trattamenti eseguiti dal Comune. Per ogni trattamento viene evidenziato:

- il nome della banca dati che raccoglie i dati personali sottoposti a trattamento;
- le sedi e gli uffici in cui avviene il trattamento;
- le finalità per le quali i dati personali vengono trattati dal Comune.

Tabella 1 - Banche dati e finalità di trattamento

Banca Dati	Sede Trattamento	Ufficio Trattamento	Finalità Trattamento
Anagrafe – Elettorale - Protocollo	Comune	Anagrafe	Istituzionale
Stato civile	Comune	Anagrafe	Istituzionale
Rapporti lavorativi	Comune/Outsourcing	Tributi - Ragioneria	Istituzionale
Tributaria	Comune/Outsourcing	Tributi	Istituzionale
Ragioneria	Comune	Segreteria - Ragioneria	Istituzionale
Archivio storico - corrente	Comune - Archivio	Archivio	Istituzionale
Polizia locale	Comune	Polizia municipale	Istituzionale
Pratiche edilizie	Comune	Tecnico	Istituzionale
Utenti servizi comunali Segreteria	Comune	Segreteria - Ragioneria	Istituzionale
Biblioteca	Piazza Buniva 7	Biblioteca	Istituzionale
Ambiente	Comune	Ambiente	Istituzionale
Videosorveglianza	Comune	Tecnico	Istituzionale

Tabella 2 per ogni banca dati sottoposta a trattamento viene evidenziata la tipologia dei dati trattati. Le tipologie prese in considerazione sono:

- **dati comuni**, sono i dati personali che permettono l'identificazione diretta dell'interessato (cfr. "dati identificativi" D. Lgs. 196/03 Art. 4 lettera c));
- **dati sensibili** (cfr. D. Lgs. 196/03 Art. 4 lettera d));
- **dati giudiziari** (cfr. D. Lgs. 196/03 Art. 4 lettera e));
- **dati sanitari**, sono dati sensibili idonei a rilevare lo stato di salute o la vita sessuale dell'interessato.

Tabella 2 - Classificazione dei dati trattati

Banca dati	Tipologia dati trattati			
	Comuni	Sensibili	Giudiziari	Sanitari
Anagrafe – Elettorale - Protocollo	X	X	X	X
Stato civile	X	X	X	X
Rapporti lavorativi	X	X		X
Tributaria	X	X	X	X
Ragioneria	X	X	X	X
Archivio storico - corrente	X	X	X	X
Polizia locale	X	X	X	X
Pratiche edilizie	X	X	X	X
Utenti servizi comunali Segreteria	X	X		
Biblioteca	X	X		
Ambiente	X			
Videosorveglianza	X			

Distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati

In Tabella viene identificato il personale del Comune che opera sulle banche dati secondo i ruoli di titolare, responsabile ed incaricato del trattamento (cfr. D. Lgs. 196/03 Art. 28, 29 e 30).

Tabella 3 - Elenco di responsabili ed incaricati al trattamento

Ruolo	Soggetto	Banche dati
Titolare	Comune di Piscina	Tutte
Responsabile	Alberto Cane	Tutte tranne Pratiche Edilizie e Polizia Municipale
Incaricata	Bianciotto Monia	Ragioneria
Incaricata	Annamaria Pecile	Anagrafe - Stato civile Archivio storico - corrente
Incaricata	Mollar Luciana	Ragioneria
Incaricata	Melisenda Cotza	Tributaria
Incaricata	Alessandra Bella	Utenti servizi comunali - Segreteria
Responsabile	Paolo Gilli	Pratiche Edilizie
Incaricato	Francesco Casati	Ambiente
Incaricato	Gangi Dino Davide	Polizia Municipale
Incaricata	Maria Michela Marcelli	Polizia Municipale
Responsabile	Alessandro Bocchino	Videosorveglianza
Incaricato	Alessandro Bocchino	Pratiche edilizie
Incaricato	Rita Ciancio	Anagrafe Archivio storico – corrente
Incaricata	Salvaggio Sonia	Biblioteca

In Tabella 4 sono elencate le banche dati che hanno trattamenti effettuati da terzi, evidenziando:

- il nome della società (ed un eventuale persona di riferimento) o della persona che prende parte al trattamento;
- la banca dati il cui trattamento è effettuato all'esterno del Comune.

E' allegata alla presente documentazione la lettera di "Nomina a Incaricato del trattamento dei dati" (allegato A.3) da far sottoscrivere nel caso di trattamenti affidati all'esterno della struttura comunale.

Tabella 2 - Elenco trattamenti in outsourcing

Ruolo	Società o persona	Banca dati
Incaricato	Alma di Mondovì	Rapporti Lavorativi
Incaricato	Equitalia Nomos Spa	Tributi (TARSU)
Incaricato	Entirev	Tributi
Incaricato	Siscom	Tutte le banche dati
Incaricato	Dedagroup	Anagrafe
Incaricato	Berno Alessandro	Tutte le banche dati

Analisi dei rischi e misure minime di sicurezza da adottare

Nei paragrafi successivi verranno discussi i rischi che incombono sui dati e verranno illustrate le misure minime da adottare per garantire l'integrità e la disponibilità dei dati.

Per ogni banca dati presente nel Comune verranno valutati:

- i rischi inerenti la protezione e la conservazione delle aree e dei locali, ovvero i pericoli legati alla perdita dei documenti in seguito a danneggiamento o accesso illecito dei locali (incendio e furto) in cui essi sono contenuti;
- i rischi inerenti l'integrità e la riservatezza delle copie cartacee dei dati, ovvero i pericoli legati ad accessi non autorizzati o ad una non adeguata conservazione delle copie cartacee;
- i rischi inerenti la riservatezza dei dati trattati in forma elettronica, ovvero i pericoli legati ad errate configurazioni dei sistemi di autenticazione e autorizzazione del sistema informativo ed alla mancanza di procedure per il rinnovo e la custodia delle credenziali d'accesso;
- i rischi inerenti l'integrità dei dati trattati in forma elettronica, ovvero i pericoli derivanti dall'intrusione nei sistemi informativi sfruttando vulnerabilità dei sistemi operativi, delle applicazioni software o della rete.

Banca dati Anagrafe – Elettorale - Protocollo

Rischi inerenti la protezione e la conservazione delle aree e dei locali

- Incendio di dati: i locali comunali sono dotati di estintori pertanto i rischi di incendio in orario lavorativo sono limitati; ciò non è vero in orario extra-lavorativo in quanto non è presente un sistema di rilevamento dei fumi ed i locali sono incustoditi.

Possibili soluzioni ai rischi rilevati

- Adozione di un sistema antincendio.

Rischi inerenti l'integrità e la riservatezza delle copie cartacee dei dati

- Nessuno

Rischi inerenti integrità e riservatezza dei dati trattati in forma elettronica

- Accesso non autorizzato su trattamenti di dati con elaboratori: la password utilizzata non è condivisa da più utenti, la lunghezza è superiore a 8 caratteri.
- Perdita di dati trattati su elaboratore: i backup sono effettuati con cadenza settimanale (automaticamente).
- Accesso abusivo a dati giuridici o sensibili: è stato introdotto un sistema di firewall.
- Sabotaggio della rete locale o di elaboratori collegati ad Internet: il software (sistema operativo) è aggiornato periodicamente.

Possibili soluzioni ai rischi rilevati

Sono state risolte tutte le problematiche che ponevano in essere rischi di perdita di dati elettronici, pertanto non si osservano né rischi né soluzioni migliori applicabili.

Banca dati Stato Civile

Rischi inerenti la protezione e la conservazione delle aree e dei locali

- Incendio di dati: i locali comunali sono dotati di estintori pertanto i rischi di incendio in orario lavorativo sono limitati; ciò non è vero in orario extra-lavorativo in quanto non è presente un sistema di rilevamento dei fumi ed i locali sono incustoditi.

Possibili soluzioni ai rischi rilevati

- Adozione di un sistema antincendio.

Rischi inerenti l'integrità e la riservatezza delle copie cartacee dei dati

- Nessuno

Rischi inerenti integrità e riservatezza dei dati trattati in forma elettronica

- Accesso non autorizzato su trattamenti di dati con elaboratori: la password utilizzata non è condivisa da più utenti, la lunghezza è superiore a 8 caratteri.
- Perdita di dati trattati su elaboratore: i backup sono effettuati con cadenza settimanale (automaticamente).
- Accesso abusivo a dati giuridici o sensibili: è stato introdotto un sistema di firewall.
- Sabotaggio della rete locale o di elaboratori collegati ad Internet: il software (sistema operativo) è aggiornato periodicamente.

Possibili soluzioni ai rischi rilevati

Sono state risolte tutte le problematiche che ponevano in essere rischi di perdita di dati elettronici, pertanto non si osservano né rischi né soluzioni migliori applicabili.

Banca dati Tributaria

Rischi inerenti la protezione e la conservazione delle aree e dei locali

- Incendio di dati: i locali comunali sono dotati di estintori pertanto i rischi di incendio in orario lavorativo sono limitati; ciò non è vero in orario extra-lavorativo in quanto non è presente un sistema di rilevamento dei fumi ed i locali sono incustoditi.

Possibili soluzioni ai rischi rilevati

- Adozione di un sistema antincendio.

Rischi inerenti l'integrità e la riservatezza delle copie cartacee dei dati

- Nessuno

Rischi inerenti integrità e riservatezza dei dati trattati in forma elettronica

- Accesso non autorizzato su trattamenti di dati con elaboratori: la password utilizzata non è condivisa da più utenti, la lunghezza è superiore a 8 caratteri.
- Perdita di dati trattati su elaboratore: i backup sono effettuati con cadenza settimanale (automaticamente).
- Accesso abusivo a dati giuridici o sensibili: è stato introdotto un sistema di firewall.
- Sabotaggio della rete locale o di elaboratori collegati ad Internet: il software (sistema operativo) è aggiornato periodicamente.

Possibili soluzioni ai rischi rilevati

Sono state risolte tutte le problematiche che ponevano in essere rischi di perdita di dati elettronici, pertanto non si osservano né rischi né soluzioni migliori applicabili.

Banca dati Ragioneria

Rischi inerenti la protezione e la conservazione delle aree e dei locali

- Incendio di dati: i locali comunali sono dotati di estintori pertanto i rischi di incendio in orario lavorativo sono limitati; ciò non è vero in orario extra-lavorativo in quanto non è presente un sistema di rilevamento dei fumi ed i locali sono incustoditi.

Possibili soluzioni ai rischi rilevati

- Adozione di un sistema antincendio.

Rischi inerenti l'integrità e la riservatezza delle copie cartacee dei dati

- Nessuno

Rischi inerenti integrità e riservatezza dei dati trattati in forma elettronica

- Accesso non autorizzato su trattamenti di dati con elaboratori: la password utilizzata non è condivisa da più utenti, la lunghezza è superiore a 8 caratteri.
- Perdita di dati trattati su elaboratore: i backup sono effettuati con cadenza settimanale (automaticamente).
- Accesso abusivo a dati giuridici o sensibili: è stato introdotto un sistema di firewall.
- Sabotaggio della rete locale o di elaboratori collegati ad Internet: il software (sistema operativo) è aggiornato periodicamente.

Possibili soluzioni ai rischi rilevati

Sono state risolte tutte le problematiche che ponevano in essere rischi di perdita di dati elettronici, pertanto non si osservano né rischi né soluzioni migliori applicabili.

Banca dati Rapporti lavorativi

Rischi inerenti la protezione e la conservazione delle aree e dei locali

- Incendio di dati: i locali comunali sono dotati di estintori pertanto i rischi di incendio in orario lavorativo sono limitati; ciò non è vero in orario extra-lavorativo in quanto non è presente un sistema di rilevamento dei fumi ed i locali sono incustoditi.

Possibili soluzioni ai rischi rilevati

- Adozione di un sistema antincendio.

Rischi inerenti l'integrità e la riservatezza delle copie cartacee dei dati

- Nessuno

Rischi inerenti integrità e riservatezza dei dati trattati in forma elettronica

- Accesso non autorizzato su trattamenti di dati con elaboratori: la password utilizzata non è condivisa da più utenti, la lunghezza è superiore a 8 caratteri.
- Perdita di dati trattati su elaboratore: i backup sono effettuati con cadenza settimanale (automaticamente).
- Accesso abusivo a dati giuridici o sensibili: è stato introdotto un sistema di firewall.
- Sabotaggio della rete locale o di elaboratori collegati ad Internet: il software (sistema operativo) è aggiornato periodicamente.

Possibili soluzioni ai rischi rilevati

Sono state risolte tutte le problematiche che ponevano in essere rischi di perdita di dati elettronici, pertanto non si osservano né rischi né soluzioni migliori applicabili.

Banca dati Pratiche edilizie

Rischi inerenti la protezione e la conservazione delle aree e dei locali

- Incendio di dati: i locali comunali sono dotati di estintori pertanto i rischi di incendio in orario lavorativo sono limitati; ciò non è vero in orario extra-lavorativo in quanto non è presente un sistema di rilevamento dei fumi ed i locali sono incustoditi.

Possibili soluzioni ai rischi rilevati

- Adozione di un sistema antincendio.

Rischi inerenti l'integrità e la riservatezza delle copie cartacee dei dati

- Nessuno

Rischi inerenti integrità e riservatezza dei dati trattati in forma elettronica

- Accesso non autorizzato su trattamenti di dati con elaboratori: la password utilizzata non è condivisa da più utenti, la lunghezza è superiore a 8 caratteri.
- Perdita di dati trattati su elaboratore: i backup sono effettuati con cadenza settimanale (automaticamente).
- Accesso abusivo a dati giuridici o sensibili: è stato introdotto un sistema di firewall.
- Sabotaggio della rete locale o di elaboratori collegati ad Internet: il software (sistema operativo) è aggiornato periodicamente.

Possibili soluzioni ai rischi rilevati

Sono state risolte tutte le problematiche che ponevano in essere rischi di perdita di dati elettronici, pertanto non si osservano né rischi né soluzioni migliori applicabili.

Banca dati Polizia Municipale

Rischi inerenti la protezione e la conservazione delle aree e dei locali

- Incendio di dati: i locali comunali sono dotati di estintori pertanto i rischi di incendio in orario lavorativo sono limitati; ciò non è vero in orario extra-lavorativo in quanto non è presente un sistema di rilevamento dei fumi ed i locali sono incustoditi.

Possibili soluzioni ai rischi rilevati

- Adozione di un sistema antincendio.

Rischi inerenti l'integrità e la riservatezza delle copie cartacee dei dati

- Nessuno

Banca dati Archivio corrente - storico

Rischi inerenti la protezione e la conservazione delle aree e dei locali

- Incendio di dati: i locali comunali sono dotati di estintori pertanto i rischi di incendio in orario lavorativo sono limitati; ciò non è vero in orario extra-lavorativo in quanto non è presente un sistema di rilevamento dei fumi ed i locali sono incustoditi.

Possibili soluzioni ai rischi rilevati

- Adozione di un sistema antincendio.

Rischi inerenti l'integrità e la riservatezza delle copie cartacee dei dati

- Nessuno (nell'archivio a parte il personale comunale non entra nessuno)

Banca dati Biblioteca

Rischi inerenti la protezione e la conservazione delle aree e dei locali

- Incendio di dati: i locali comunali sono dotati di estintori pertanto i rischi di incendio in orario lavorativo sono limitati; ciò non è vero in orario extra-lavorativo in quanto non è presente un sistema di rilevamento dei fumi ed i locali sono incustoditi.

Possibili soluzioni ai rischi rilevati

- Adozione di un sistema antincendio.

Rischi inerenti l'integrità e la riservatezza delle copie cartacee dei dati

- Nessuno

Rischi inerenti integrità e riservatezza dei dati trattati in forma elettronica

- Accesso non autorizzato su trattamenti di dati con elaboratori: la password utilizzata non è condivisa da più utenti, la lunghezza è superiore a 8 caratteri.
- Perdita di dati trattati su elaboratore: i backup sono effettuati con cadenza settimanale (automaticamente).
- Accesso abusivo a dati giuridici o sensibili: è stato introdotto un sistema di firewall.
- Sabotaggio della rete locale o di elaboratori collegati ad Internet: il software (sistema operativo) è aggiornato periodicamente.

Possibili soluzioni ai rischi rilevati

Sono state risolte tutte le problematiche che ponevano in essere rischi di perdita di dati elettronici, pertanto non si osservano né rischi né soluzioni migliori applicabili.

Banca dati Utenti servizi comunali Segreteria

Rischi inerenti la protezione e la conservazione delle aree e dei locali

- Incendio di dati: i locali comunali sono dotati di estintori pertanto i rischi di incendio in orario lavorativo sono limitati; ciò non è vero in orario extra-lavorativo in quanto non è presente un sistema di rilevamento dei fumi ed i locali sono incustoditi.

Possibili soluzioni ai rischi rilevati

- Adozione di un sistema antincendio.

Rischi inerenti l'integrità e la riservatezza delle copie cartacee dei dati

- Nessuno

Rischi inerenti integrità e riservatezza dei dati trattati in forma elettronica

- Accesso non autorizzato su trattamenti di dati con elaboratori: la password utilizzata non è condivisa da più utenti, la lunghezza è superiore a 8 caratteri.
- Perdita di dati trattati su elaboratore: i backup sono effettuati con cadenza settimanale (automaticamente).
- Accesso abusivo a dati giuridici o sensibili: è stato introdotto un sistema di firewall.
- Sabotaggio della rete locale o di elaboratori collegati ad Internet: il software (sistema operativo) è aggiornato periodicamente.

Possibili soluzioni ai rischi rilevati

Sono state risolte tutte le problematiche che ponevano in essere rischi di perdita di dati elettronici, pertanto non si osservano né rischi né soluzioni migliori applicabili.

Banca dati Videosorveglianza

Sul territorio del Comune di Piscina è attivo un sistema di videosorveglianza. Il sistema è regolamentato dal "Regolamento per la disciplina della videosorveglianza".

Telecamera	Ubicazione	Angolo di ripresa	Caratteristiche tecniche
1	Viale Rimembranza	Ingresso principale cimitero	Fissa
2	Viale Rimembranza	Ingresso secondario cimitero	Fissa
3	Viale Rimembranza	Chiesa San Rocco	Fissa
4	Piazza Eugenia Corti	Piazza	Fissa
5	Piazza Eugenia Corti	Piazza	Fissa
6	Via Umberto I incrocio via Airasca	Ecopunto	Fissa
7	Viale Rimembranza	Parcheggio cimitero	Fissa

Tutte le telecamere indicate consentono riprese notturne.

Descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento

I backup delle banche dati sono effettuati dai relativi responsabili del servizio su supporti removibili (floppy disk o CD scrivibili) con cadenza settimanale.

Nel caso si verificasse la perdita dei dati i responsabili sarebbero in grado di ripristinarli in un tempo massimo di sette giorni, anche tramite il ricorso ad un tecnico abilitato.

Descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare

L'assegnazione di incarichi esterni a terzi, che verranno nominati incaricati al trattamento, è subordinata ad una dichiarazione degli stessi di attenersi al D.Lgs. 30/06/03 n.196 e di essere a conoscenza delle norme specifiche del regolamento comunale.

Allegata alla presente documentazione la lettera "Nomina a Incaricato al Trattamento dei dati" da far sottoscrivere nel caso di trattamenti affidati all'esterno della struttura Comunale (presente nel CDROM allegato sotto "Lettere\Lettera incarico a terzi.doc").

Criteri da adottare per la cifratura o per la separazione dei dati personali idonei a rivelare lo stato di salute e la vita sessuale dagli altri dati personali dell'interessato

È prevista la formalizzazione di una procedura con la quale i dati personali idonei a rivelare lo stato di salute o la vita sessuale dell'individuo saranno conservati separatamente dagli altri, nel caso in cui siano su supporto cartaceo essi saranno tenuti in appositi armadi e/o cassetti muniti di serratura e saranno accessibili ai soli addetti individuati.