COMUNE DI PONZA

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI PERSONALI

Data Protection Impact Assessment (DPIA)

ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (GDPR)

Titolare del trattamento	**Comune di Ponza**
Dati Completi Reperibili al link:	***https://www.comune.ponza.lt.it/trattamento-dati/***
Data redazione	**Giugno 2026**
Versione documento	**Nuova stesura - 1.0**
Stato	**APPROVATO CON DELIBERA DI GIUNTA 104/2026**

1. PREMESSA E BASE NORMATIVA

La presente Valutazione di Impatto sulla Protezione dei Dati (DPIA - Data Protection Impact Assessment) è redatta dal Comune di Ponza, in qualità di Titolare del trattamento, in conformità all'art. 35 del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio (GDPR).

La DPIA costituisce uno strumento fondamentale per valutare, prima dell'avvio di un trattamento che possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, la necessità e la proporzionalità del trattamento stesso, nonché per gestire i rischi per i diritti e le libertà degli interessati.

1.1 Quadro normativo di riferimento

- Regolamento (UE) 2016/679 (GDPR) - artt. 35 e 36
- D.Lgs. 30 giugno 2003, n. 196 (Codice della Privacy) come modificato dal D.Lgs. 101/2018
- Linee guida WP29/EDPB n. 248 rev. 01 sulle DPIA
- Provvedimento del Garante per la protezione dei dati personali n. 467 del 11/10/2018 (elenco trattamenti soggetti a DPIA)
- D.Lgs. 18 agosto 2000, n. 267 (TUEL) - Ordinamento degli enti locali
- D.Lgs. 7 marzo 2005, n. 82 (CAD) - Codice dell'Amministrazione Digitale

1.2 Soggetti coinvolti

Titolare del trattamento	Comune di Ponza - P.IVA 80012560594 - Via Roma, 1 - 04027 Ponza (LT)
Sindaco (legale rappresentante)	Francesco Ambrosino
Responsabile della Protezione dei Dati (DPO)	Sorrentino Giacomo
Responsabile del procedimento	Francesco Ambrosino
Referente interno alla redazione	Filippo Conte

2. DESCRIZIONE DEL TRATTAMENTO

Il Comune di Ponza, ente locale situato nell'arcipelago ponziano, svolge molteplici attività di trattamento di dati personali nell'esercizio delle proprie funzioni istituzionali. La presente DPIA si riferisce all'insieme dei trattamenti relativi ai seguenti servizi e attività amministrative:

2.1 Finalità del trattamento

Il Comune di Ponza tratta dati personali per le seguenti categorie di finalità:

N.	Finalità	Base giuridica (art. 6 GDPR)	Categorie particolari (art. 9)
1	Anagrafe, stato civile e servizi demografici	Obbligo legale (art. 6 c.1 lett. c)	No
2	Tributi locali (IMU, TARI, TOSAP)	Obbligo legale (art. 6 c.1 lett. c)	No
3	Gestione del personale dipendente	Contratto / Obbligo legale	Sì (salute, sindacali)
4	Servizi sociali e assistenza alla persona	Obbligo legale / Interesse pubblico	Sì (salute, origine etnica)
5	Edilizia, urbanistica e SUAP	Obbligo legale (art. 6 c.1 lett. c)	No
6	Gestione protocollo e atti amministrativi	Obbligo legale (art. 6 c.1 lett. c)	Eventualmente sì
7	Videosorveglianza pubblica	Interesse pubblico (art. 6 c.1 lett. e)	No
8	Portale istituzionale e servizi digitali (SPID/CIE)	Obbligo legale / Contratto	No
9	Gestione contabilità e appalti pubblici	Obbligo legale (art. 6 c.1 lett. c)	No
10	Turismo, porto e demanio marittimo	Obbligo legale / Interesse pubblico	No

2.2 Categorie di dati personali trattati

Il Comune tratta le seguenti categorie di dati:

Dati comuni (art. 4 GDPR)

- Dati anagrafici e identificativi (nome, cognome, codice fiscale, data e luogo di nascita)
- Dati di contatto (indirizzo di residenza/domicilio, numero di telefono, indirizzo e-mail)
- Dati economici e fiscali (reddito, patrimonio immobiliare, ISEE)
- Dati relativi a procedimenti amministrativi, concessioni, autorizzazioni
- Immagini (videosorveglianza, fotografie per documenti)
- Dati di navigazione e log informatici

Dati particolari (art. 9 GDPR)

- Dati relativi alla salute (servizi sociali, personale, invalidità)
- Dati sull'origine razziale o etnica (servizi sociali, anagrafe stranieri)
- Dati biometrici (firma digitale, sistemi di accesso)
- Dati relativi all'appartenenza sindacale (gestione del personale)
- Dati relativi a condanne penali e reati (art. 10 GDPR - specifici procedimenti)

2.3 Categorie di interessati

- Cittadini residenti nel Comune di Ponza e nell'arcipelago ponziano

- Turisti e visitatori (utenti stagionali - popolazione estiva significativa)
- Dipendenti e collaboratori dell'ente
- Imprenditori, operatori economici e titolari di concessioni demaniali
- Fornitori e appaltatori
- Minori (in relazione a servizi scolastici e sociali)
- Soggetti vulnerabili (anziani, disabili, persone in stato di bisogno)

2.4 Tecnologie e sistemi utilizzati

- Software gestionale per la Pubblica Amministrazione (es. Halley, TeamSystem, Maggioli o equivalente)
- Sistema di protocollo informatico (PEC istituzionale)
- Portale istituzionale con accesso tramite SPID/CIE
- Sistema di videosorveglianza del territorio e delle aree portuali
- Infrastruttura cloud (eventualmente in uso presso il Comune)
- Piattaforma ANPR (Anagrafe Nazionale della Popolazione Residente)

3. NECESSITÀ E PROPORZIONALITÀ

Ai sensi dell'art. 35, paragrafo 7, lettera b) del GDPR, la DPIA deve valutare la necessità e la proporzionalità dei trattamenti rispetto alle finalità perseguite.

3.1 Necessità del trattamento

I trattamenti descritti nella presente DPIA sono necessari in quanto derivano direttamente dall'esercizio di funzioni istituzionali attribuite dalla legge agli enti locali. Il Comune di Ponza non dispone di margini discrezionali per esimersi dall'esecuzione dei trattamenti obbligatori previsti dalla normativa vigente.

Per le attività discrezionali (es. iniziative turistiche, comunicazione istituzionale), il trattamento è limitato allo stretto necessario per il perseguimento delle finalità dichiarate.

3.2 Principio di minimizzazione

Il Comune di Ponza si impegna ad adottare le seguenti misure di minimizzazione:

- Raccolta dei soli dati strettamente necessari per ciascuna finalità amministrativa
- Conservazione dei dati per il periodo minimo previsto dalla normativa e dai piani di conservazione documentale
- Pseudonimizzazione e anonimizzazione dei dati quando possibile (es. statistiche, pubblicazioni)
- Revisione periodica degli archivi per eliminare dati non più necessari

3.3 Periodi di conservazione

Categoria di dati	Periodo di conservazione	Riferimento normativo
Dati anagrafici e stato civile	Illimitata (atti pubblici)	D.P.R. 396/2000
Dati tributari	10 anni dalla definizione	D.P.R. 600/1973
Documenti contabili e appalti	10 anni + eventuale contenzioso	D.Lgs. 267/2000
Dati del personale	Durata rapporto + 10 anni	CCNL Enti Locali
Immagini videosorveglianza	Massimo 7 giorni (48 h aree porto)	Provv. Garante 8/4/2010
Pratiche edilizie e urbanistiche	Illimitata (atti amminist.)	D.P.R. 380/2001
Dati servizi sociali	5 anni dalla chiusura pratica	D.Lgs. 196/2003
Log informatici e accessi	6 mesi (12 mesi con motivazione)	Provv. Garante 2007

4. IDENTIFICAZIONE E VALUTAZIONE DEI RISCHI

La valutazione dei rischi viene effettuata considerando la probabilità e la gravità dei rischi per i diritti e le libertà degli interessati, tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento.

4.1 Metodologia di valutazione

La valutazione del rischio residuo è effettuata secondo la seguente scala:

Livello di rischio	Probabilità	Impatto	Punteggio
BASSO	Improbabile (1)	Trascurabile (1)	1-2
MEDIO	Possibile (2)	Significativo (2)	3-4
ALTO	Probabile (3)	Grave (3)	6-9

4.2 Scenario di rischio e misure di mitigazione

Rischio identificato	Prob.	Impatto	Livello	Misure di mitigazione
Accesso non autorizzato ai sistemi informatici (attacco hacker/ransomware)	2	3	ALTO	Firewall, antivirus, autenticazione a 2 fattori, backup, piano di disaster recovery
Perdita o distruzione accidentale dei dati	2	3	ALTO	Backup giornalieri su server ridondanti, piano BCP, procedure di ripristino testate
Accesso abusivo da parte di dipendenti (insider threat)	2	3	ALTO	Profili di accesso differenziati (RBAC), log degli accessi, formazione, codice di condotta
Violazione dati personali in videosorveglianza	1	3	MEDIO	Accesso limitato al sistema, monitoraggio degli accessi, conservazione max 7 giorni
Comunicazione illecita a terzi di dati sensibili	2	3	ALTO	Accordi di riservatezza, formazione, verifica identità del richiedente, procedure formali
Trattamento eccedente le finalità dichiarate	2	2	MEDIO	Registro dei trattamenti aggiornato, audit interni, informative agli interessati
Mancato rispetto dei diritti degli interessati	2	2	MEDIO	Procedure interne per la gestione delle richieste, tempi di risposta monitorati
Trasferimento dati extra-UE non conforme	1	3	MEDIO	Verifica sistematica degli strumenti cloud utilizzati, clausole contrattuali standard
Phishing e ingegneria sociale verso dipendenti	3	2	ALTO	Formazione periodica, simulazioni di phishing, policy sull'uso degli strumenti IT
Violazione sicurezza negli applicativi web/portale	2	2	MEDIO	Test di penetrazione periodici, aggiornamento software, HTTPS obbligatorio, WAF

5. MISURE DI SICUREZZA ADOTTATE

Il Comune di Ponza ha adottato, ai sensi dell'art. 32 del GDPR, misure tecniche e organizzative adeguate a garantire un livello di sicurezza appropriato al rischio.

5.1 Misure tecniche

Sicurezza informatica

- Sistemi di autenticazione sicura con password policy e, ove possibile, autenticazione multi-fattore (MFA)
- Antivirus e sistemi EDR (Endpoint Detection & Response) aggiornati
- Firewall perimetrale e sistemi IDS/IPS
- Cifratura dei dati in transito (TLS 1.2/1.3) e a riposo per dati particolari
- Segmentazione della rete informatica (separazione reti amministrative e guest)
- Backup automatici giornalieri con verifica dell'integrità e copia off-site
- Gestione delle patch e degli aggiornamenti di sicurezza (patch management)

Controllo degli accessi

- Sistema di profilazione degli accessi basato sul ruolo (RBAC - Role Based Access Control)
- Registrazione dei log di accesso con conservazione per almeno 6 mesi
- Revisione periodica dei profili di accesso e revoca tempestiva a fine rapporto
- Accesso fisico controllato ai server room e agli archivi cartacei (chiavi, badge, CCTV)

Continuità operativa

- Piano di Business Continuity (BCP) e Disaster Recovery aggiornato
- Test periodici di ripristino dei backup
- Ridondanza dei sistemi critici

5.2 Misure organizzative

- Nomina formale del Responsabile della Protezione dei Dati (DPO)
- Registro dei trattamenti aggiornato ai sensi dell'art. 30 GDPR
- Designazione per iscritto degli incaricati al trattamento e dei Responsabili esterni (art. 28 GDPR)
- Formazione obbligatoria annuale del personale in materia di protezione dei dati
- Procedure interne per la gestione dei data breach (notifica al Garante entro 72 ore)
- Procedure per la gestione delle richieste degli interessati (accesso, rettifica, cancellazione, opposizione)
- Informative privacy complete e aggiornate per tutte le tipologie di trattamento
- Policy di utilizzo accettabile degli strumenti IT aziendali
- Audit interni periodici sulla conformità al GDPR
- Valutazione preventiva dei fornitori e responsabili del trattamento (vendor assessment)

5.3 Misure specifiche per categorie particolari di dati

Per i trattamenti che coinvolgono dati particolari (art. 9 GDPR), vengono adottate misure aggiuntive:

- Cifratura end-to-end delle comunicazioni contenenti dati sanitari
- Accesso limitato ai soli operatori dei servizi sociali e sanitari competenti
- Conservazione separata dei dati particolari rispetto agli altri dati
- Utilizzo di pseudonimizzazione nelle fasi di elaborazione statistica
- Accordi specifici con soggetti sanitari coinvolti nel trattamento

6. DIRITTI DEGLI INTERESSATI

Il Comune di Ponza garantisce il pieno esercizio dei diritti riconosciuti agli interessati dagli artt. 15-22 del GDPR.

Diritto	Contenuto	Modalità di esercizio
Diritto di accesso (art. 15)	Ottenere conferma del trattamento e copia dei dati	Istanza scritta all'ufficio protocollo o via PEC
Diritto di rettifica (art. 16)	Correggere dati inesatti o incompleti	Istanza scritta con documentazione
Diritto alla cancellazione (art. 17)	Cancellazione ove non vi sia obbligo di conservazione	Istanza motivata - valutazione caso per caso
Diritto di limitazione (art. 18)	Limitare il trattamento in specifici casi	Istanza scritta con indicazione dei motivi
Diritto alla portabilità (art. 20)	Ricevere i dati in formato strutturato (solo base contrattuale/consenso)	Applicabile limitatamente ai servizi digitali
Diritto di opposizione (art. 21)	Opporsi al trattamento per motivi legittimi	Istanza motivata - valutazione con DPO
Diritto di reclamo (art. 77)	Proporre reclamo al Garante Privacy	www.garanteprivacy.it

Le richieste degli interessati sono gestite dall'Ufficio competente in collaborazione con il DPO e devono ricevere risposta entro 30 giorni, prorogabili a 90 giorni in caso di complessità, con comunicazione all'interessato.

Punto di contatto per l'esercizio dei diritti:

- Indirizzo PEC istituzionale: ufficiosegreteria@pec.it
- Indirizzo mail: urp@comune.ponza.lt.it
- Indirizzo: Piazza Carlo Pisacane, 1 - 04027 Ponza (LT)
- E-mail DPO: sorrentino.gioacomo@gmail.com

7. TRASFERIMENTI VERSO PAESI TERZI

Il Comune di Ponza non effettua, in linea di principio, trasferimenti sistematici di dati personali verso Paesi al di fuori dello Spazio Economico Europeo (SEE). Tuttavia, l'utilizzo di taluni strumenti informatici (piattaforme SaaS, servizi cloud, videoconferenze) potrebbe comportare trasferimenti accidentali o tecnicamente necessari verso server ubicati fuori dall'UE.

Per tali fattispecie, il Comune adotta le seguenti misure di garanzia:

- Verifica preventiva della sede dei server dei fornitori di servizi cloud (preferenza per data center EU)
- Inserimento nelle convenzioni con i fornitori delle Clausole Contrattuali Standard (SCC) adottate dalla Commissione UE
- Verifica dell'adeguatezza del Paese destinatario ai sensi dell'art. 45 GDPR
- Mappatura annuale degli strumenti utilizzati e aggiornamento del registro dei trattamenti

8. CONSULTAZIONE DEL DPO E PARERE

Il Responsabile della Protezione dei Dati (DPO) del Comune di Ponza è stato consultato nella fase di redazione della presente DPIA, in conformità all'art. 35, par. 2 del GDPR.

DPO consultato	Sì
Data della consulta	*17/06/2026*
Parere del DPO	*Favorevole (Protocollo Comune di Ponza N.11590/2026)*
Osservazioni del DPO	*1. mantenere costantemente aggiornate le misure tecniche ed organizzative adottate;* *2. procedere alla revisione periodica della DPIA in occasione di modifiche sostanziali del trattamento, delle tecnologie impiegate o del contesto normativo di riferimento;* *3. garantire la continua formazione del personale autorizzato al trattamento;* *4. monitorare periodicamente l'efficacia delle misure di sicurezza implementate;*

9. PIANO DI AZIONE E RIESAME

Il seguente piano di azione definisce le misure da implementare per ridurre i rischi residui identificati nella presente DPIA.

Azione	Responsabile	Scadenza	Priorità
Adozione piano di formazione annuale GDPR per tutti i dipendenti	DPO / Risorse Umane	Entro 3 mesi	ALTA
Implementazione MFA su tutti i sistemi gestionali	Responsabile IT	Entro 6 mesi	ALTA
Aggiornamento e verifica del Registro dei Trattamenti (art. 30)	DPO	Entro 2 mesi	ALTA
Revisione e aggiornamento di tutte le informative privacy	DPO / Uffici	Entro 4 mesi	MEDIA
Procedura per la gestione delle violazioni di dati (data breach)	DPO / IT	Entro 2 mesi	ALTA
Test di penetrazione e vulnerability assessment sui sistemi	Responsabile IT	Semestrale	MEDIA
Verifica contrattuale dei responsabili del trattamento (art. 28)	DPO / Ufficio Appalti	Entro 6 mesi	ALTA
Mappatura strumenti cloud con verifica trasferimenti extra-UE	DPO / IT	Entro 3 mesi	MEDIA
Test di ripristino backup e aggiornamento piano DR	Responsabile IT	Semestrale	MEDIA
Revisione annuale della presente DPIA	DPO / Titolare	Annuale	BASSA

9.1 Periodicità di riesame

La presente DPIA è soggetta a riesame nei seguenti casi:

- Annualmente, a prescindere da variazioni del contesto
- In caso di variazioni significative delle modalità o finalità del trattamento
- In caso di adozione di nuove tecnologie o sistemi informatici
- A seguito di un data breach che abbia coinvolto i trattamenti oggetto della presente DPIA
- A seguito di modifiche normative rilevanti
- Su indicazione del DPO o del Garante per la Protezione dei Dati Personali

10. CONSULTAZIONE PREVENTIVA DEL GARANTE

Ai sensi dell'art. 36 del GDPR, qualora dalla valutazione del rischio residuo emerga che il trattamento presenterebbe ancora un rischio elevato in assenza di misure adottate dal titolare per attenuarlo, il titolare del trattamento è tenuto a consultare preventivamente l'Autorità di controllo competente (Garante per la Protezione dei Dati Personali).

Valutazione	Esito
Necessità di consultazione preventiva del Garante	NON NECESSARIA - i rischi residui sono stati ridotti a livello accettabile con le misure adottate
Motivazione	Le misure tecniche e organizzative descritte nella sezione 5 risultano adeguate a ridurre i rischi a un livello accettabile. Nessun trattamento presenta rischi residui elevati non mitigabili

Qualora in futuro venissero introdotti nuovi trattamenti ad alto rischio (es. sistemi di riconoscimento facciale, profilazione sistematica, sorveglianza biometrica), il Comune di Ponza procederà a una nuova DPIA specifica e valuterà la necessità di consultazione preventiva del Garante.

11. APPROVAZIONE E FIRME

La presente Valutazione di Impatto sulla Protezione dei Dati è stata redatta e approvata dai soggetti di seguito indicati.

Ruolo	Nome e Cognome	Firma e Data
Titolare del trattamento (Sindaco)	Ambrosino Francesco	Firmato digitalmente ai sensi del D.Lgs. 82/2005 (CAD) s.m.i. e norme collegate.
Responsabile della Protezione dei Dati (DPO)	Sorrentino Giacomo	Firmato digitalmente ai sensi del D.Lgs. 82/2005 (CAD) s.m.i. e norme collegate.
Responsabile del Procedimento	Ambrosino Francesco	Firmato digitalmente ai sensi del D.Lgs. 82/2005 (CAD) s.m.i. e norme collegate.
Responsabile IT / Sistemi informativi	Ambrosino Francesco	Firmato digitalmente ai sensi del D.Lgs. 82/2005 (CAD) s.m.i. e norme collegate.

Documento firmato digitalmente ai sensi del CAD e delle normative ad esso connesse.
L'originale è conservato informaticamente.

Ponza, Giugno 2026

ALLEGATI

Alla presente DPIA sono allegati i seguenti documenti (da compilare a cura degli uffici competenti):

- Allegato A - Registro dei Trattamenti (art. 30 GDPR)
- Allegato B - Organigramma della protezione dei dati
- Allegato C - Elenco dei Responsabili del trattamento (art. 28 GDPR)
- Allegato D - Modulo per la gestione delle richieste degli interessati
- Allegato E - Procedura per la gestione dei Data Breach
- Allegato F - Policy di utilizzo accettabile degli strumenti IT
- Allegato G - Verbale di consultazione del DPO
- Allegato H - Piano di formazione annuale del personale