Comune di Sant'Omero

Provincia di Teramo

"***Registro dei trattamenti***"

previsto dal RGPD – UE 2016/679 del 27 aprile 2016

(*Regolamento Generale sulla Protezione dei Dati*).

- Prima approvazione: Deliberazione della Giunta comunale n. 21 del 30/03/2020
- Aggiornamento: Deliberazione della Giunta comunale n. ..... del ...../...../.....

.

Sommario

Premessa

*Con apposita determinazione del Responsabile del settore, questa amministrazione ha incaricato la ditta Grafiche E. Gaspari srl di fornire una consulenza generale e un affiancamento agli uffici comunali per gli adempimenti conseguenti all'entrata in vigore del Regolamento UE 2016/679 (RGPD) del 27 aprile 2016 relativo alla "**Protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati**", che sono entrati in vigore il 25 maggio 2018.*

Nello svolgimento di questo incarico, questa amministrazione ha nominato, come Responsabile della protezione dei dati personali, la ditta Grafiche E. Gaspari srl, con apposita comunicazione al Garante della Privacy, sotto riportata.

Nell'ambito di detta fornitura la ditta Grafiche E. Gaspari srl ha nominato come suo referente per questa amministrazione il dott. Agostino Pasquini, nato a Lunano (PS) il 02/04/1966, CF PSQGTN66D02E743V, autore di numerose pubblicazioni sulla privacy ed esperto della materia, che si avvale della collaborazione del dott. Paolo Russomanno. Il Dott. Agostino Pasquini ha svolto presso il Comune di Sant'Omero un'iniziativa di confronto e formazione il giorno 05/06/2019. In quell'occasione sono state fornite le principali nozioni relative alla tematica della privacy, così come configurata dal Regolamento Europeo (RGPD) e dal Codice della privacy (d.lgs. 30/06/2003, n. 196, come da ultimo modificato e integrato dal d.lgs. 10/08/2018, n. 101), rispondendo inoltre a quesiti e dubbi operativi dei presenti.

Il Registro è un documento fondamentale contenente le principali informazioni (specificatamente individuate dall'art. 30 del RGPD) relative alle operazioni di trattamento svolte dal titolare e, se nominato, dal responsabile del trattamento (sul registro del responsabile). Costituisce uno dei principali elementi di accountability (responsabilizzazione) del titolare, in quanto strumento idoneo a fornire un quadro aggiornato dei trattamenti in essere all'interno della propria organizzazione, indispensabile per ogni attività di valutazione o analisi del rischio e dunque preliminare rispetto a tali attività.

La Giunta Comunale provvederà ad adottare formalmente questo documento, predisposto in collaborazione con il Responsabile della Protezione dei dati personali.

È programmato almeno un aggiornamento ogni anno, con le stesse modalità. Il Registro dei trattamenti è infatti un documento di censimento e analisi dei trattamenti effettuati e, in quanto tale, deve essere mantenuto costantemente aggiornato poiché il suo contenuto deve sempre corrispondere all'effettività dei trattamenti posti in essere. Qualsiasi cambiamento, in particolare in ordine alle modalità, finalità, categorie di dati, categorie di interessati, deve essere immediatamente inserito nel Registro, dando conto delle modifiche sopravvenute.

Una copia di questo documento verrà formalmente consegnato al Responsabile Comunale per la Prevenzione della Corruzione e Trasparenza, affinché ne tenga conto nell'aggiornamento annuale del relativo piano.

Comunicazione al Garante della Privacy della nomina del RPD

GPDP.Ufficio.Registro RPD.0001277.28/01/2019

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Comunicazione dei dati di contatto del responsabile della protezione dei dati

(art. 37, par. 7 del RGPD e art. 28, c. 4 del D.Lgs. 51/2018)

A. Dati del soggetto che effettua la comunicazione

Cognome : LUZII Nome : ANDREA
E-mail : sindaco@comune.santomero.te.it
nella sua qualita' di ☒ rappresentante legale o ☐ delegato del rappresentante legale
dichiara di aver preso visione dell'informativa sul trattamento dei dati personali ☒
comunica i seguenti dati ai sensi e per gli effetti di cui all'art. 37, par. 7, del RGPD:

B. Dati del TITOLARE/RESPONSABILE DEL TRATTAMENTO

Il Titolare/Responsabile del trattamento e':

☐ Censito nell' Indice nazionale dei domicili digitali delle imprese e dei professionisti *(www.inipec.gov.it - art. 6-bis CAD)*

☒ Censito nell' Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi *(www.indicepa.gov.it - art. 6-ter CAD)*

☐ Non e' censito in nessuno dei due precedenti indici

Denominazione : COMUNE DI SANT'OMERO
Codice Fiscale/P.IVA : 82002660676
Stato : ITALIA
Indirizzo : VIA VITTORIO VENETO N 52
Citta' : SANT'OMERO
CAP : 64027 Provincia : TE
Telefono : 086188098
E-mail : segreteria@comune.santomero.te.it
PEC : segreteria@pec.comune.santomero.te.it

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

C. RESPONSABILE DELLA PROTEZIONE DEI DATI

Tipo di designazione del Responsabile della protezione dei dati personali

☐ interno ☒ esterno

Il Responsabile della protezione dei dati personali e':

☐ persona fisica ☒ persona giuridica

Dati del Responsabile della protezione dei dati

Denominazione : GRAFICHE E. GASPARI S.R.L.
Codice Fiscale/P.IVA : 00089070403 Soggetto privo di cf/piva ☐
Stato : ITALIA
Indirizzo : VIA M. MINGHETTI 18
Citta' : GRANAROLO DELL'EMILIA
CAP : 40057 Provincia : BO
Telefono : 051763201
E-mail : privacy@gaspari.it
PEC : privacy@pec.egaspari.net

Soggetto individuato quale referente per il titolare/responsabile

Cognome : PASQUINI
Nome : AGOSTINO

Dati di contatto

Telefono : 051763201
Mobile : 3298076127
E-mail : privacy@gaspari.it
PEC : privacy@pec.egaspari.net

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

D. PUBBLICAZIONE DEI DATI DI CONTATTO

I dati di contatto del RPD sono resi pubblici dal titolare/responsabile mediante:

☒ pubblicazione sul sito web (indicare l'indirizzo del sito su cui e' possibile reperire l'informazione) : www.comune.santomero.te.it
☐ Altro (specificare)

Tabella – A: I servizi ed uffici del comune, suddivisi per aree/settori omogenei[1], in cui sussistono necessariamente, perché obbligatorie per legge, delle banche dati personali

COD.	Denominazione della banca dati personale	Barrare se non gestita	Barrare se gestita all' esterno
Banche dati personali degli "affari generali" e risorse umane			
A01	Anagrafe dei dipendenti e degli amministratori		
A02	Contratti e ufficio legale - Protocollo		
A03	Dati trattati dall' O.I.V. o dal nucleo di valutazione		X
A04	Dati trattati dal Responsabile Comunale per la prevenzione della corruzione e trasparenza		
A05	Dati trattati dal Responsabile del Servizio Prevenzione e Protezione e dal medico del lavoro		X
A06	Dati trattati dall'organismo di disciplina	X	
A07	Dati personali trattati dal "Responsabile della protezione dei dati"		X
Banche dati personali dei servizi demografici			
A08	Anagrafe comunale o anagrafe nazionale (APR – ANPR)		
A09	Dinamica demografica statistica e censimenti		
A10	Leva militare e servizio civile volontario	X	
A11	Stato civile		
A12	Elettorato attivo e passivo		
A13	Carta d'identità (cartacea ed elettronica)		
A14	Polizia mortuaria e servizi cimiteriali		
Banche dati personali dei servizi alla persona			
A15	Assistiti e beneficiari di provvidenze		X
A16	Asili nido e scuole dell'infanzia		X
A17	Scuola dell'obbligo – centri giovani		
Banche dati personali dei servizi di vigilanza e controllo			
A18	Polizia municipale/locale – polizia giudiziaria - Verbali e sistema sanzionatorio		
A19	Videosorveglianza	X	
Banche dati personali dei servizi alle imprese e al patrimonio edile privato			
A20	Sportello unico per le attività produttive		
A21	Sportello unico per l'edilizia		
Banche dati personali dei servizi culturali, sportivi e turistici			
A22	Ufficio sport, manifestazioni e turismo	X	
A23	Biblioteca comunale – cultura	X	
Banche dati personali dei servizi finanziari			
A24	Servizi finanziari – fornitori – destinatari di pagamenti vari		
A25	Tributi		X
Banche dati personali dei servizi al terzo settore e alle attività di democrazia diretta			
A26	Protezione civile e attività di cittadinanza attiva		X
A27	Associazioni di volontariato, di promozione sociale e libero associazionismo – comitati		X
A28	Organismi di democrazia diretta: petizioni, consulte, referendum e consultazioni pubbliche	X	
A29	Comunicazione istituzionale		
Banche dati personali dei servizi ai proprietari di animali			
A30	Gestione animali d'affezione (cani, gatti ecc.)	X	

[1] La suddivisione in settori, non necessariamente rispetta l'assetto del comune disciplinato da regolamenti o provvedimenti interni, ma è utile per il lavoro che segue.

Tabella – B: Le banche dati personali ulteriori a quelle obbligatorie

COD.	Denominazione della banca dati personale	Eventuali riferimenti normativi o estremi di regolamento locale
B01	Farmacia comunale	Art.9, L. 02/04/1968, n. 475
B02		
B03		
B04		
B05		
B06		
B07		
B08		
B09		
B10		

Tabella – C: Gli applicativi informatici (procedure) con cui vengono gestite le banche di dati personali

COD.	Denominazione dell'applicativo informatico e/o della ditta fornitrice	Codice delle banche dati personali (tabelle **A** e **B**) che vengono gestiti con l'applicativo	Barrare se la ditta esporta i dati su server esterni
C01	Halley Informatica S.r.l.	A02 - A04 - A12 - A15 - A16 - A17 - A24 - A20 - A21 - A25	X
C02	Actainfo di Addari Igino s.a.s.	A02 - A12 - A15 - A16 - A17 - A24 - A25 - A27	
C03	Alfa Communication Srl	A29	X
C04			
C05			
C06			
C07			
C08			
C09			
C10			

Tabella – D: Gli apparati fisici, analogici ed informatici con cui vengono gestiti i dati personali, nelle sedi comunali

COD.	Tipologia dell'apparato	Codice delle banche dati personali (tabelle A e B) che vengono gestiti con l'apparato	Quantità totali di apparati di questo tipo in comune
D01	Armadi o schedari chiusi a chiave o custoditi in locali chiusi a chiave o ad accesso controllato	A18	1
D02	Armadi o schedari **non** chiusi a chiave o **non** custoditi in locali chiusi a chiave o **non** ad accesso controllato	A01 - A02 - A04 - A05 - A12 - A14 - A15 - A16 - A17 - A24 - A25 - A26 - A27	18
D03	Server di rete o Nas o apparati simili, protetti da sistemi logici ad accesso limitato e/o profilato (ID + PW o simili)		
D04	Server di rete o Nas o apparati simili, **non** protetti da sistemi logici ad accesso limitato e/o **non** profilato (ID + PW o simili)	A01 - A02 - A04 - A12 - A16 - A17 - A18 - A20 - A21 - A24 - A25 - A27	1
D05	PC o terminali connessi ad una intranet comunale protetta da sistemi logici ad accesso limitato e/o profilato (ID + PW o simili)	A01 - A02 - A04 - A12 - A15 - A16 - A17 - A20 - A21 - A24 - A25 - A27	17
D06	PC o terminali **non** connessi ad una intranet comunale, ma protetti da sistemi logici ad accesso limitato e/o profilato		
D07	PC o terminali connessi ad una intranet comunale **non** protetta da sistemi logici ad accesso limitato e/o profilato (ID + PW o simili)		
D08	TABLET, SMARTPHONE, APPARATI WI FI, APPARATI RIMOVIBILI		
D09	Servizi in cloud o similari (gestiti in Unione Europea)		
D10	Servizi in cloud o similari (**non** gestiti in Unione Europea)		

Tabella – E: Elenco dei soggetti (amministratori, dipendenti, collaboratori diretti) che operano sulle banche dati personali secondo un vincolo di subordinazione diretta al comune

Cognome e nome	Codice delle banche dati personali (tabelle **A** e **B**) che vengono gestiti dal soggetto	Codice degli apparti a cui ha accesso (tabella **D**)
Luzii Andrea – Sindaco	A08 - A11	D02 – D05
Clementoni Vincenzina - Istruttore	A02 - A27	D02 – D05
Cretone Gigino - Istruttore	A14 - A20 - A21 - A26	D02 – D05
Di Ubaldo Francesca - Istruttore	A24	D02 – D05
Gatti Grazietta - Istruttore	A12 - A16 - A17	D02 – D05
Ianni Margherita - Istruttore	A15	D02 – D05
Marcellini Sandro – Responsabile	A05 - A14 - A20 - A21 - A26 - A29	D02 – D05
Pace Vito– Responsabile	A18	D01 – D05
Giovannini Franco - Responsabile	A18	D01
Di Pierdomenico Paolo – Responsabile	A01 - A02 - A04 - A08 - A09 - A11 - A12 - A13 - A14 - A15 - A16 - A17 - A24 - A25 - A27	D02 – D05
Ricci Ilario - Istruttore	A02	D02 – D05
Serranò Lodovico	A02 - A24	
Cimiconi Michela – Staff	A24	D02 – D05
Butini Francesco (Farmacia)	B01	D02

Tabella – F: Elenco dei Responsabili del trattamento che operano sulle banche dati personali secondo un atto di natura convenzionale (contratto di servizio, concessione o simili), senza vincolo di subordinazione

Cognome e nome o ragione sociale	Codice delle banche dati personali (tabelle **A** e **B**) che vengono gestiti dal soggetto	Codice degli apparti a cui ha accesso (tabella **D**), anche da remoto	Barrare se utilizza suoi apparati fuori dal controllo diretto del comune
Halley Informatica S.r.l.	A02 - A04 - A12 - A15 - A16 - A17 - A24 - A20 - A21 - A25	D04 - D05	
Dott. Gloria Piscina	A05		
Alfa Communication Srl	A29	D05	

Tabella – G: Misure organizzative e/o di autovalutazione per la sicurezza e integrità dei dati personali

Per stessa ammissione del Garante della privacy e secondo lo spirito che sottende a tutto il RGPD, dove si parla spesso di accountability – responsabilizzazione, anche questo registro non deve essere un mero adempimento, ma un'occasione di valutazione delle misure necessarie per mettere in sicurezza e trattare secondo le disposizioni di legge o regolamento, i dati personali del comune.

In quest'ottica risulta utile fare un'autovalutazione sull'attuazione di queste misure:

G01 - Adozione delle misure fisiche di protezione degli archivi cartacei (*chiavi agli armadi, chiavi e sistemi antintrusione agli uffici, consapevolezza di dover chiudere al sicuro i dati …*)

Parziale: 5,26 %

G02 - Conoscenza delle linee guida di AGID per il "disaster recovery" e la continuità operativa

No

G03 - Adozione di misure antiintrusione sui server locali e remoti

Si

G04 - Adozione di misure di sicurezza sulla rete interna e sulla rete internet

Parziale: 50%

G05 - Strategie di pseudonimizzazione dei dati, specie quando dagli stessi possano desumersi, anche in via indiretta, le condizioni di disagio sociale o le condizioni di salute

Parziale: 50%

G06 - Responsabilizzazione degli operatori sulle "politiche di sicurezza e salvaguardia dei dati personali" (*divieto di usare propri device, accessi profilati ecc.*)

Si

G07 - Definizione di obblighi precisi per il personale interno e i soggetti esterni coinvolti nel trattamento dei dati personali

No

G08 - Conoscenza delle modalità di gestione dei data-breach (violazione dei dati)

Si

Indicazioni preliminari alla valutazione d'impatto del trattamento

La valutazione di impatto del trattamento (D.P.I.A., Data Protection Impact Assessment) è un onere a carico del titolare del trattamento (art. 35 G.D.P.R.), col quale si assicura trasparenza e protezione nelle operazioni di trattamento dei dati personali. Il titolare effettua tramite tale strumento l'analisi dei rischi derivanti dai trattamenti di dati personali posti in essere. Il rischio, secondo le previsioni della normativa in materia di privacy, è "uno scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini di gravità e probabilità» per i diritti e le libertà (Linee guida del Gruppo di lavoro Articolo 29 WP248rev.1).

La valutazione del rischio dovrà portare il titolare a decidere in autonomia, a seguito di un confronto con il Responsabile per la Protezione dei Dati e secondo il principio di accountability (responsabilizzazione), se sussistono rischi elevati inerenti il trattamento stesso. Se dovessero risultare sussistenti rischi per le libertà e i diritti degli interessati, sarà necessario individuare le misure specifiche richieste per attenuare o eliminare tali rischi.

Il par. 9 dell'art. 35 del G.D.P.R. prevede anche la possibilità che il titolare consulti gli interessati coinvolti, per valutazioni sull'eventuale invasività del trattamento.

La valutazione di impatto va sviluppata solo per particolari trattamenti, in base a precisi criteri:

- *il trattamento determina una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici;*
- *il trattamento riguarda dati sensibili o giudiziari su larga scala;*
- *il trattamento riguarda la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.*

Le Linee guida del Gruppo di lavoro Articolo 29 WP248rev.1 hanno specificato nove parametri utili all'individuazione dei casi di necessità della D.P.I.A., mentre il Garante italiano ha predisposto un elenco pubblico di tipologie di trattamenti per i quali si rende necessaria la D.P.I.A, pubblicato con provvedimento dell'11 ottobre 2018.

In riferimento alla peculiare situazione dell'Ente locale, che per i suoi stessi scopi istituzionali raccoglie, tratta e conserva grandi quantità di dati personali si è ritenuto, in accordo con il D.P.O, di sviluppare una complessiva valutazione del rischio dei trattamenti compiuti a livello comunale, adeguandola alle più sviluppate previsioni sul tema a livello europeo.
Particolare attenzione sarà poi dedicata a quei trattamenti che le autorità di controllo sulla privacy hanno individuato quali particolarmente delicate.

Tale compito, da svilupparsi successivamente all'approvazione del presente registro, costituirà un elemento di quel vero e proprio "ciclo della privacy" che deve corrispondere ad un'azione costante e crescente del titolare (in confronto con il D.P.O.) volta a garantire una sempre maggiore aderenza del trattamento dei dati compiuto in comune con i principi e le prescrizioni della nuova normativa in materia.

Avvertenza
Questo registro è stato redatto ispirandosi al modello di registro per le PMI proposto dal Garante della Privacy italiano e dalle tabelle prodotte dal software PIA, dell'autority francese, adattando tutti questi schemi, anche in forma semplificata, ai trattamenti di dati effettuati dai comuni, quasi esclusivamente disposti per legge; dunque sui trattamenti disposti per legge, serve una valutazione "semplificata" essendo gli stessi "obbligatori".
Nei prossimi mesi sarà necessario estrapolare dai dati raccolti ed elaborati, quanto serve per fare la valutazione di impatto. Al termine della valutazione di impatto tutto il registro avrà una completa coerenza ed efficacia.