Consiglio di Bacino Verona Sud

Provincia di Verona

"***Registro dei trattamenti***"

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

(*Regolamento Generale sulla Protezione dei Dati*).

- Prima approvazione: Determina n. 16 del 18/09/2019
- Aggiornamento: Determina 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 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. Russomanno ha svolto presso l'ente una giornata di confronto e formazione in data 27/08/2019. 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.

Il Direttore del Consiglio di Bacino Verona Sud 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 dell'Ente 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.0007190.30/05/2019

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Comunicazione dei dati di contatto del Responsabile della Protezione dei Dati - RPD

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

A. Dati del soggetto che effettua la comunicazione

Il sottoscritto Cognome : FRANZONI Nome : MARCO
E-mail : info@bacinovrsud.it
nella sua qualità di ☒ rappresentante legale o ☐ delegato del rappresentante legale
dichiara di aver preso visione dell'informativa sul trattamento dei dati personali ☒
e consapevole delle conseguenze previste dall'art. 168 del D.Lgs. 196/2003 circa la falsità nelle comunicazioni al Garante, comunica i seguenti dati ai sensi e per gli effetti di cui all'art. 37, par. 7, del RGPD:

A1. Tipo di comunicazione

Tipo di comunicazione dei dati di contatto del RPD:

☐ Nuova comunicazione
☒ Variazione di una comunicazione - Protocollo n.: 20180034663
☐ Revoca di una comunicazione

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

B. Titolare/Responsabile del trattamento

1) Il Titolare/Responsabile del trattamento è:

☐ Censito nell'Indice nazionale dei domicili digitali delle imprese e dei professionisti
(INI-PEC www.inipec.gov.it - art. 6-bis Codice Amministrazione Digitale - D.Lgs n. 82/2005)

☒ Censito nell'Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi *(IPA www.indicepa.gov.it - art. 6-ter Codice Amministrazione Digitale - D.Lgs n. 82/2005)*

☐ Non è censito in nessuno dei due precedenti indici

2) Dati del Titolare/Responsabile del trattamento:

Denominazione : CONSIGLIO DI BACINO VERONA SUD
Codice Fiscale : 93264700233
Stato : ITALIA
Provincia : VR Comune : BOVOLONE CAP : 37051
Indirizzo : PIAZZA SCIPIONI 1
Telefono : 0456949164
E-mail :
PEC : protocollo@pec.bacinovrsud.it

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

C. Responsabile della Protezione dei Dati

1) Tipo di designazione del Responsabile della Protezione dei Dati

☐ interno ☒ esterno

2) Il Responsabile della protezione dei dati è:

☐ persona fisica ☒ persona giuridica

3) Dati del Responsabile della Protezione dei Dati

Denominazione : GRAFICHE E. GASPARI SRL
P.IVA : 00089070403
Stato : ITALIA
Provincia : BO Comune : GRANAROLO DELL'EMILIA CAP : 40057
Indirizzo : VIA M MINGHETTI 18
Telefono : 051763201
E-mail : privacy@gaspari.it
PEC : privacy@pec.egaspari.net

Soggetto individuato quale referente per il Titolare/Responsabile

Cognome : PASQUINI
Nome : AGOSTINO

4) Dati di contatto

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

Tabella - A: I servizi ed uffici dell'Ente, 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		
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		
A07	Dati personali trattati dal "Responsabile della protezione dei dati"		
Banche dati personali dei servizi finanziari			
A24	Servizi finanziari - fornitori - destinatari di pagamenti vari		
Banche dati personali dei servizi al terzo settore e alle attività di democrazia diretta			
A29	Comunicazione istituzionale		

[1] La suddivisione in settori, non necessariamente rispetta l'assetto dell'Ente 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	Gestione posta elettronica	
B02	Gestione server	

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 Srl	A01 - A02 - A03 - A04 - A07 - A24 - A29	
C02	Comunicanet di Ferrarini Renzo	B01	X
C03	Brembenet di Scamperle Nella	B02	
C04	Studio Bonfante	A01	X
C05	FIT-CISL Federazione Italiana Trasporti	A01	X
C06	Intesa Sanpaolo S.p.A. (Servizio di Tesoreria)	A01 - A24	X
C07	ACCATRE Srl	A01 - A02 - A03 - A04 - A07 - A24 - A29	

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 nell'Ente
D01	Armadi o schedari chiusi a chiave o custoditi in locali chiusi a chiave o ad accesso controllato	A1 - A24	1
D02	Armadi o schedari **non** chiusi a chiave o **non** custoditi in locali chiusi a chiave o **non** ad accesso controllato		
D03	Server di rete o Nas o apparati simili, protetti da sistemi logici ad accesso limitato e/o profilato (ID + PW o simili)	A1 - A24	1
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)		
D05	PC o terminali connessi ad una intranet comunale protetta da sistemi logici ad accesso limitato e/o profilato (ID + PW o simili)	A1 - A24	2
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)	A24	1
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 all'ente

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**)
Chiaramonte Marta	A01 - A02 - A04 - A07 - A24 - A29 - B01	D01 - D03 - D05 - D09
Mirandola Sabina	A01 - A02 - A04 - A07 - A24 - A29 - B01	D01 - D03 - D05 - D09
Ballarin Alessandro	A01 - A02 - A04 - A07 - A24 - A29	D01 - D03 - D05 - D09
Lavanda Barbara	A01 - A02 - A04 - A07 - A24 - A29 - B01	D01 - D03 - D05 - D09
Zerbinati Gianni	A01 - A02 - A04 - A07 - A24 - A29	D01 - D03 - D05 - D09

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 dell'Ente
Halley Informatica Srl	A01 - A02 - A03 - A04 - A07 - A24 - A29	X	X
Comunicanet di Ferrarini Renzo	B01	X	
Brembenet di Scamperle Nella	B02	X	
Studio Bonfante	A01		
FIT-CISL Federazione Italiana Trasporti	A01		
Intesa Sanpaolo S.p.A. (Servizio di Tesoreria)	A01 - A24		X
RSPP (in fase di nomina)			
Medico competente (in fase di nomina)			
Grafiche E.Gaspari Srl			X
ACCATRE Srl		X	X

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 dell'Ente.

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 …*)

Si

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

Si

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

Si

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

No

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 nell'Ente 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