

# UNIONE DI COMUNI APPENNINO PISTOIESE

(Abetone, Cutigliano, Piteglio, Sambuca P.se, San Marcello P.se)

## COPIA DELLA

### DELIBERA DI CONSIGLIO NUMERO 15 DEL 30/06/2018

**OGGETTO: Regolamento di attuazione del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali**

L'anno DUEMILADICIOTTO e questo giorno TRENTA del mese di GIUGNO alle ore 10.45 presso la sala consiliare del palazzo comunale di San Marcello Pistoiese, si e' riunito il Consiglio dell'Unione di Comuni Montani Appennino Pistoiese, in sessione ORDINARIA ed in PRIMA convocazione, sotto la presidenza del Sig. MARMO LUCA nella sua qualita' di PRESIDENTE.

All'appello risultano presenti n. 6 consiglieri ed assenti, sebbene debitamente convocati, n. 3, come segue:

Nominativo Consigliere	Stato	Nominativo Consigliere	Stato
MARMO LUCA	Pres.	BRACCESI TOMMASO	Ass.
BARTOLI DANIELA	Pres.	MICHELETTI FABIO	Pres.
DUCCI VENUSIA	Pres.	TADDEI CHRISTIAN	Ass.
PETRUCCI DIEGO	Pres.	FRONTI KELLY MARIA	Ass.
BACCI GABRIELE	Pres.		

Assiste il Vice Segretario provvisorio dell'Unione DOTT. TESI GIULIA il quale provvede alla redazione del presente verbale

IL PRESIDENTE

constatato il numero legale degli intervenuti ai fini della legittimità dell'adunanza, dichiara aperta la seduta e designa quali scrutatori i Sigg. DUCCHI VENUSIA, BACCI GABRIELE, BARTOLI DANIELA, ed il Consiglio passa alla discussione degli oggetti posti all'ordine del giorno adottando la seguente deliberazione

## IL CONSIGLIO DELL'UNIONE

RICHIAMATO l'art. 42, c.2, lett. a), D.Lgs. 18 agosto 2000 n.267;

### PRESO ATTO:

- Che il Parlamento europeo ed il Consiglio in data 27.4.2016 hanno approvato il Regolamento UE 679/2016 (GDPR- General Data Protection Regulation) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che abroga la direttiva 95/46/CE e che mira a garantire una disciplina uniforme ed omogenea in tutto il territorio dell'Unione europea;
- Che il testo, pubblicato nella Gazzetta Ufficiale dell'Unione Europea (GUUE) il 4 maggio 2016, diventerà definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal 25 maggio 2018, dopo un periodo di transizione di due anni, in quanto non richiede alcuna forma di legislazione applicativa o attuativa da parte degli stati membri;
- Che il Garante per la protezione dei dati personali ha emanato una Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali che intende offrire un panorama delle principali problematiche che i soggetti pubblici, oltre alle imprese, dovranno tenere presenti in vista della piena applicazione del Regolamento, prevista il 25 maggio 2018;
- Che ai sensi dell'art.13 della Legge n.163/2017 il Governo è stato delegato ad adottare, entro sei mesi dalla sua entrata in vigore, uno o più decreti legislativi al fine di adeguare il quadro normativo nazionale alle disposizioni del Regolamento (UE) 2016/679 del 27 aprile 2016 di che trattasi;

### RILEVATO:

- Che le norme introdotte dal Regolamento UE 2016/679 si traducono in obblighi organizzativi, documentali e tecnici che tutti i Titolari del trattamento dei dati personali devono, fin da subito, considerare e tenere presenti per consentire la piena e consapevole applicazione del nuovo quadro normativo in materia di privacy entro il 25 maggio 2018;
- Che appare necessario ed opportuno stabilire modalità organizzative, misure procedurali e regole di dettaglio, finalizzate anche ad omogeneizzare questioni interpretative, che permettano a questo Ente di poter agire con adeguata funzionalità ed efficacia nell'attuazione delle disposizioni introdotte dal nuovo Regolamento UE;
- Visto lo schema di Regolamento allegato;

RITENUTO pertanto opportuno procedere alla sua approvazione per permettere a questa Amministrazione di provvedere con immediatezza all'attuazione del Regolamento UE 2016/679;

VISTO il parere di regolarità tecnica reso ai sensi dell'art. 49, Tuel e dato atto che la presente delibera non necessita di parere di regolarità contabile non comportando impegno di spesa né diminuzione di entrata;

Che votazione unanime espressa nelle forme di legge  
Tanto premesso,

## DELIBERA

1) Di approvare il Regolamento attuativo del Regolamento UE 2016/679 in materia di protezione dati personali, che consta di n.11 articoli e n.3 schede che viene allegato al presente atto per costituirne parte integrante e sostanziale.

2) Di dare atto che con successivi provvedimenti, adottati dai soggetti competenti di questa Amministrazione,

si procederà secondo la disciplina contenuta nel presente atto ed in conformità a quanto stabilito nel Regolamento UE 2016/679 ed in particolare:

- alla nomina dei Responsabili del trattamento;
- alla designazione del Responsabile della Protezione Dati;
- all'istituzione dei registri delle attività di trattamento;
- a mettere in atto misure tecniche e organizzative adeguate per garantire ed essere in grado di dimostrare che i trattamenti dei dati personali vengono effettuati in conformità alla disciplina europea;
- all'aggiornamento della documentazione in essere nell'Ente in relazione ai trattamenti dei dati personali;

3) di dichiarare la presente deliberazione immediatamente eseguibile ai sensi dell' art. 134, comma 4, D.Lgs. n. 267/200

IL PRESIDENTE

F.to

MARMO LUCA

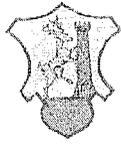
IL SEGRETARIO

F.to

DOTT. TESI GIULIA

## UNIONE DI COMUNI MONTANI APPENNINO PISTOIESE

Tra i Comuni di Abetone Cutigliano, San Marcello Piteglio, Sambuca Pistoiese



**OGGETTO:** Regolamento dell'Unione di Comuni Montani Appennino Pistoiese di attuazione del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

### Parere del Segretario dell'Ente

Il sottoscritto, in qualità di Segretario dell'Unione di Comuni Montani Appennino Pistoiese, ai fini e per gli effetti dell'art. 147 bis del D.Lgs. n. 267/00 e s.m.i.

ESPRIME

Parere favorevole in ordine alla regolarità tecnica della proposta di delibera di Consiglio in oggetto.

San Marcello Pistoiese, 15.06.2018

Il Segretario

Dott.ssa Francesca Merlini

Unione Comuni Apennino Pistoiese - Unione Municipi di Pistoia, Pescina, Pescina  
Paolina, Pescina Paolina, Pescina Paolina, Pescina Paolina, Pescina Paolina



Via Pietro Leopoldo 18/24 - 51028 San Marcello Pistoiese - [unionecomuniapenninopistoiese@pec.it](mailto:unionecomuniapenninopistoiese@pec.it)  
C.F. : 90054150472

## Regolamento per l'attuazione del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali

# UNIONE DI COMUNI MONTANI APPENNINO PISTOIESE

Tra i Comuni di Abetone Cutigliano, San Marcello Piteglio e Sambuca Pistoiese



Via Pietro Leopoldo 10/24 51028 San Marcello Pistoiese – [unionecomuniappenninopistoiese@pec.it](mailto:unionecomuniappenninopistoiese@pec.it)  
C.F. : 90054130472

Art. 1 - Oggetto

Art. 2 - Titolare del trattamento

Art. 3 - Finalità del trattamento

Art. 4 - Responsabile del trattamento

Art. 5 - Responsabile della protezione dati

Art. 6 - Sicurezza del trattamento

Art. 7 - Registro delle attività di trattamento

Art. 8 - Registro delle categorie di attività trattate

Art. 9 - Valutazione d'impatto sulla protezione dei dati

Art. 10 - Violazione dei dati personali

Art. 11 - Rinvio

Allegati

A) schema di registro attività di trattamento

B) schema di registro categorie attività di trattamento

C) schema di registro unico di trattamento



Via Pietro Leopoldo 10/24 - 51028 San Marcello Pistoiese - [unionecomuniappenninopistoiese@pec.it](mailto:unionecomuniappenninopistoiese@pec.it)  
C.F. : 90054130472

## Art. 1

### Oggetto

1. Il presente Regolamento ha per oggetto misure procedurali e regole di dettaglio ai fini della migliore funzionalità ed efficacia dell'attuazione del Regolamento europeo (General Data Protection Regulation del 27 aprile 2016 n. 679, di seguito indicato con "RGPD", Regolamento Generale Protezione Dati), relative alle protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione di tali dati, nell'Unione di Comuni montani Appennino Pistoiese.

## Art.2

### Titolare del trattamento

1. L'Unione di Comuni montani Appennino P.se (d'ora in avanti denominata "Unione"), rappresentata ai fini previsti dal RGPD dal Presidente pro tempore, è il Titolare del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee (di seguito indicato con "Titolare"). Il Presidente può delegare le relative funzioni ai Responsabili di Posizione Organizzativa in possesso di adeguate competenze.

2. 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.

3. Il Titolare mette in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme al RGPD.

Le misure sono definite 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 stabiliti dagli articoli 15-22 RGPD, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio.

Gli interventi necessari per l'attuazione delle misure sono considerati nell'ambito della programmazione operativa (DUP), di bilancio e di Peg, previa apposita analisi preventiva della situazione in essere, tenuto conto dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi dallo stesso derivanti, aventi probabilità e gravità diverse per i diritti e la libertà delle persone fisiche.

4. Il Titolare adotta misure appropriate per fornire all'interessato:

a) le informazioni indicate dall'art. 13 RGPD, prima dei dati personali diventando obbligatorie, e, in caso di mancato consenso;

# UNIONE COMUNI APPENNINI PISTOIESE

## UNIONE DI COMUNI DELLA PROVINCIA DI PISTOIA



Via Pietro Leopoldo 10/24 - 51028 San Marcello Pistoiese - [unionescomuniappenninipistoiese@pec.it](mailto:unionescomuniappenninipistoiese@pec.it)  
C.F. : 90054180472

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

5. Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti o la libertà delle persone fisiche, il Titolare deve effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito indicata con "DPIA") ai sensi dell'art. 35, RGPD, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento, tenuto conto di quanto indicato dal successivo art. 3.

6. Il Titolare, inoltre, prevede a:

a) designare i Responsabili del trattamento nelle persone dei Responsabili di Posizione Organizzativa e dei Funzionari delle singole strutture in cui si articola l'organizzazione dell'Ente, che sono preposti al trattamento dei dati contenuti nelle banche dati esistenti nelle articolazioni organizzative di loro competenza. Per il trattamento di dati il Titolare può avvalersi anche di soggetti pubblici o privati;

b) nominare il Responsabile della protezione dei dati;

c) nominare quale Responsabile del trattamento i soggetti pubblici o privati affidatari di attività e servizi per conto dell'Amministrazione, relativamente alle banche dati gestite da soggetti esterni all'Ente in virtù di convenzioni, di contratti, o di incarichi professionali o altri strumenti giuridici consentiti dalla legge, per la realizzazione di attività connesse alle attività istituzionali;

7. Nel caso di esercizio associato di funzioni e servizi, nonché per i compiti la cui gestione è affidata all'Unione da enti ed organismi statali o regionali, allorché due o più titolari determinano congiuntamente, mediante accordo, le finalità ed i mezzi del trattamento, si realizza la contitolarieté di cui all'art. 26 RGPD. L'accordo definisce la 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 dalle normative specificatamente applicabili; l'accordo può individuare un punto di contatto comune per gli interessati.

8. L'Unione favorisce l'adesione ai codici di condotta elaborati dalle 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 dimostrare il concreto rispetto da parte del Titolare e dei Responsabili del trattamento.

## Art.2

### Finalità del trattamento

1. I trattamenti sono compiuti al fine per le seguenti finalità:



Via Pietro Leopoldo 40/24 - 51028 San Marcello Pistoiese - [unione.comuniappenninopistoiese@pec.it](mailto:unione.comuniappenninopistoiese@pec.it)  
C.F. : 90054130472

a) l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri. Rientrano in questo ambito i trattamenti compiuti per:

- l'esercizio delle funzioni amministrative che riguardano la popolazione ed il territorio, precipuamente nei settori organici dei servizi alla persona ed alla comunità, dell'assetto ed utilizzazione del territorio e dello sviluppo economico;
- la gestione dei servizi elettorali, di stato civile, di anagrafe, di base militare e di statistica, ove le funzioni fossero trasferite da Comuni aderenti;
- l'esercizio di ulteriori funzioni amministrative per servizi di competenza statale affidate all'Unione in base alla vigente legislazione. La finalità del trattamento è stabilita dalla fonte normativa che lo disciplina;

b) l'adempimento di un obbligo legale al quale è soggetta l'Unione. La finalità del trattamento è stabilita dalla fonte normativa che lo disciplina;

c) l'esecuzione di un contratto con soggetti interessati;

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

#### Art.4

##### Responsabile del trattamento

1. Un Responsabile di Posizione Organizzativa dell'Ente, è nominato unico Responsabile del trattamento di tutto lo banche dati personali esistenti nell'articolazione organizzativa di rispettiva competenza. Il Responsabile unico deve essere in grado di offrire garanzie sufficienti in termini di conoscenza specialistica, esperienza, capacità ed affidabilità, per mettere in atto le misure tecniche e organizzative di cui all'art. 6 rivolto a garantire che i trattamenti siano effettuati in conformità al RGPD.

2. I dipendenti dell'Unione, Responsabili del trattamento, sono designati, di norma, mediante decreto di incarico del Presidente, nel quale sono tassativamente disciplinati:

- la materia trattata, la durata, la natura e la finalità del trattamento o dei trattamenti assegnati;
- il tipo di dati personali oggetto di trattamento e la categoria di interessati;
- gli obblighi ed i diritti del Titolare del trattamento.



Via Pietro Leopoldo 19/23 - 51028 San Marcello Pistoiese - [unionecomuniapenninopistoiese@pec.it](mailto:unionecomuniapenninopistoiese@pec.it)  
C.F. : 90054130472

Tale disciplina può essere contenuta anche in apposita convenzione o contratto da stipularsi fra il Titolare e ciascun responsabile designato.

3. Il Titolare può avvalersi, per il trattamento di dati, anche sensibili, di soggetti pubblici o privati che, in qualità di responsabili del trattamento, forniscano le garanzie di cui al comma 1, 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.

4. Gli atti che disciplinano il rapporto tra il Titolare ed il Responsabile del trattamento devono in particolare contenere quanto previsto dall'art. 28, p. 3, RGPD; tali atti possono anche basarsi su clausole contrattuali tipo adottate dal Garante per la protezione dei dati personali oppure dalla Commissione europea.

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 ed 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, anzitutto quelli specificati per iscritto nell'atto di designazione, ed in particolare provvede:

- alla tenuta del registro delle categorie di attività di trattamento svolte per conto del Titolare;
- all'adozione di idonee misure tecniche e organizzative adeguate per garantire la sicurezza dei trattamenti;
- alla sensibilizzazione ed alla formazione del personale che partecipa ai trattamenti ed alle connesse attività di controllo;
- alla designazione del titolare della protezione dei dati (DPO), in accordo con il Garante del TIB (art. 37).

Unione Comuni Appennini Pistoiesi  
Via Fiesco Tolosani, 10 - 51022 San Marcello Pistoiese - Pistoia - Toscana - Italia



Via Fiesco Tolosani 10/24 - 51022 San Marcello Pistoiese - [unionecomuniappenninipistoiese@pec.it](mailto:unionecomuniappenninipistoiese@pec.it)  
C.F. : 90054130472

- ad assistere il Titolare nella conduzione della valutazione dell'impatto sulla protezione dei dati (di seguito indicata con "DPIA") fornendo allo stesso ogni informazione di cui è in possesso;

- 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, nel caso che il Titolare stesso ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati.

## Art.3

### Responsabile della protezione dati

1. Il Responsabile della protezione dei dati (in seguito indicato con "RPD") è individuato in una figura unica, scelta alternativamente tra un dipendente di ruolo dell'Unione, ovvero un professionista.

Il RPD è incaricato dei seguenti compiti:

a) informare e fornire consulenza al Titolare ed al Responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal RGPD e dalle altre normative relative alla protezione dei dati. In tal senso il RPD può indicare al Titolare e/o al Responsabile del trattamento i settori funzionali ai quali riservare un audit interno o esterno in tema di protezione dei dati, le attività di formazione interna per il personale che tratta dati personali, e a quali trattamenti dedicare maggiori risorse e tempo in relazione al rischio riscontrato;

b) sorvegliare l'osservanza del RGPD e delle altre normative relative alla protezione dei dati, fermo restando la responsabilità del Titolare e del Responsabile del trattamento;

Fanno parte di questi compiti la raccolta di informazioni per individuare i trattamenti a rischio, l'analisi e la verifica dei trattamenti in termini di loro conformità, l'attività di informazione, consulenza e indirizzo nei confronti del Titolare e del Responsabile del trattamento;

c) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare e dal Responsabile del trattamento;

d) fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e consigliarne lo svolgimento. Il Titolare, in particolare, si consulta con il RPD in merito a: se condurre o meno una DPIA; quale metodologia adottare nel condurre una DPIA; se condurre la DPIA con le risorse interne ovvero externalizzandola; quali rischi/risorse applicare, come procedure formali o informali, per attenuare i rischi dello stesso interessato; se la DPIA sia



Via Pietro Leopoldo 10/24 - I-50028 San Marcello Pistoiese - [unionecomuniappenninopistoiese@pec.it](mailto:unionecomuniappenninopistoiese@pec.it)  
C.F. : 80054330472

stata condotta correttamente o meno e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al RGPD;

e) cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 RGPD, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione. A tali fini il nominativo del RPD è comunicato dal Titolare e/o dal Responsabile del trattamento al Garante;

f) la tenuta dei registri di cui ai successivi artt. 7 e 8;

g) altri compiti e funzioni a condizione che il Titolare o il Responsabile del trattamento si assicurino che tali compiti e funzioni non diano adito a un conflitto di interessi.

L'assenza di conflitti di interessi è strettamente connessa agli obblighi di indipendenza del RPD.

2. Il Titolare ed il Responsabile del trattamento assicurano che il RPD sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. A tal fine:

- il RPD è invitato a partecipare alle riunioni di coordinamento dei Responsabili di P.O. che abbiano per oggetto questioni inerenti la protezione dei dati personali;

- il RPD deve disporre tempestivamente di tutte le informazioni pertinenti sulle decisioni che impattano sulla protezione dei dati, in modo da poter rendere una consulenza idonea, scritta od orale;

- Il parere del RPD sulle decisioni che impattano sulla protezione dei dati è obbligatorio ma non vincolante. Nel caso in cui la decisione assunta determina condotte difformi da quelle raccomandate dal RPD, è necessario motivare specificamente tale decisione;

- il RPD deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.

3. Nello svolgimento dei compiti affidatigli il RPD deve debitamente considerare i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo. In tal senso il RPD:

a) procede ad una mappatura delle aree di attività valutandone il grado di rischio in termini di protezione dei dati;

b) definisce un ordine di priorità dell'attività da svolgere - ovvero un piano annuale di attività - presentandone nelle aree di attività che presentano maggiori rischi in termini di protezione dei dati, da essere realizzate in base ad un calendario da concordare con il Responsabile del trattamento.

## Art. 10 - Funzione di Responsabile del Protezione dei Dati (RPD)



Via Pietro Leopoldo 10/24 - 51028 San Marcello Pistoiese - [unione.comuniappenninopistoiese@pec.it](mailto:unione.comuniappenninopistoiese@pec.it)  
C.F. : 90054130472

4. Il RPD dispone di autonomia e risorse sufficienti a svolgere in modo efficace i compiti attribuiti, tenuto conto delle dimensioni organizzative o delle capacità di bilancio dell'Ente.

5. La figura di RPD è incompatibile con chi determina le finalità od i mezzi del trattamento; in particolare, risultano con la stessa incompatibili:

- il Responsabile per la prevenzione della corruzione o per la trasparenza;
- il Responsabile del trattamento;
- qualunque incarico o funzione che comporta la determinazione di finalità o mezzi del trattamento.

6. Il Titolare ed il Responsabile del trattamento forniscono al RPD le risorse necessarie per assolvere i compiti attribuiti e per accedere ai dati personali ed ai trattamenti. In particolare è assicurato al RPD:

- supporto attivo per lo svolgimento dei compiti da parte dei Responsabili di P.O. e della Giunta comunale, anche considerando l'attuazione delle attività necessarie per la protezione dati nell'ambito della programmazione operativa (DUP), di bilancio, di Peg e di Piano della performance;
- tempo sufficiente per l'espletamento dei compiti affidati al RPD;
- supporto adeguato in termini di risorse finanziarie, infrastrutture (sede, attrezzature, strumentazione) e, ove opportuno, personale;
- comunicazione ufficiale della nomina a tutto il personale, in modo da garantire che la sua presenza e le sue funzioni siano note all'interno dell'Ente;
- accesso garantito ai vertici funzionali dell'Ente o ad altri funzionari, informazioni o input essenziali.

7. Il RPD opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti; in particolare, non deve ricevere istruzioni in merito al loro svolgimento né sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati.

Il RPD non può essere rimesso o penalizzato dal Titolare e dal Responsabile del trattamento per l'adempimento dei propri compiti.

Perme restando l'indipendenza nello svolgimento di detti compiti, il RPD riferisce direttamente al Titolare - Presidente o suo delegato - ed al Responsabile del trattamento.



Via Pietro Leopoldo 10/34 - 51028 San Marcello Fisioloiese - [unioecomuniappenninofrosinolese@pec.it](mailto:unioecomuniappenninofrosinolese@pec.it)  
C.F. : 90054130472

Nei casi in cui siano rilevate dal RPD o sottoposte alla sua attenzione decisioni incompatibili con il RGPD e con le indicazioni fornite dallo stesso RPD, quest'ultimo è tenuto a manifestare il proprio dissenso, comunicandolo al Titolare ed al Responsabile del trattamento.

## Art.6

### Sicurezza del trattamento

1. L'Unione e ciascun Responsabile del trattamento mettono in atto misure tecniche ed organizzative adeguate 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: la pseudonimizzazione; la minimizzazione; la cifratura dei dati personali; la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico; 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 dal Servizio cui è preposto ciascun Responsabile del trattamento:

- sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antifittazione; altro);

- misure antifisaccia; sistemi di rilevazione di intrusioni; 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 o ad un meccanismo di certificazione approvato.

5. L'Unione 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.



Via Pietro Leopoldo 10/24 - 51028 San Marcello Pistoiese -- [unione.comuni.appenninopistoiese@pec.it](mailto:unione.comuni.appenninopistoiese@pec.it)  
C.F. : 90054330472

6. I nominativi ed i dati di contatto del Titolare, del o dei Responsabili del trattamento e del Responsabile della protezione dati sono pubblicati sul sito istituzionale del Comune, sezione Amministrazione trasparente.

7. Restano in vigore le misure di sicurezza attualmente previste per i trattamenti di dati sensibili per finalità di rilevante interesse pubblico nel rispetto degli specifici regolamenti attuativi (ex artt. 20 e 22, D.Lgs. n. 193/2006).

#### Art.7

##### Registro delle attività di trattamento

1. Il Registro delle attività di trattamento svolte dal Titolare del trattamento reca almeno le seguenti informazioni:

a) il nome ed i dati di contatto dell'Unione, del Presidente e/o del suo Delegato ai sensi del precedente art.2, eventualmente del Conditore del trattamento, del RPD;

b) le finalità del trattamento;

c) la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;

d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;

e) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;

f) ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

g) il richiamo alle norme di sicurezza tecniche ed organizzative del trattamento adottate, come da precedente art.6.

2. Il Registro è tenuto dal Titolare ovvero dal soggetto dallo stesso delegato ai sensi del precedente art. 2, presso gli uffici della struttura organizzativa dell'Unione in forma telematica o cartacea, secondo lo schema allegato A al presente Regolamento; nello stesso possono essere inserite ulteriori informazioni tenuto conto delle dimensioni organizzative dell'Ente.

3. Il Titolare del trattamento può decidere di affidare al RPD il compito di tenere il Registro, sotto la responsabilità del medesimo Titolare.

4. Il Titolare può decidere di tenere un Registro unico dei trattamenti che contiene le informazioni di cui al comma precedente a quella di cui al precedente art. 6, adottando comunque la tipologia di dati ed i dati personali che risultano dalle diverse finalità di cui è prevista l'adozione di misure di



Via Pietro Leopoldo 10/2A - 51028 San Marcello Pistoiese - [g.jonecornuniappanni@pec.it](mailto:g.jonecornuniappanni@pec.it)  
C.F. : 90054150472

caso, il Titolare delega la sua tenuta al Responsabile unico del trattamento di cui al precedente art. 4 o, comunque, ad un solo Responsabile del trattamento, ovvero può decidere di affidare tale compito al RPD, sotto la responsabilità del medesimo Titolare. Ciascun Responsabile del trattamento ha comunque la responsabilità di fornire prontamente e correttamente al soggetto preposto ogni elemento necessario alla regolare tenuta ed aggiornamento del Registro unico.

#### Art.8

##### Registro delle categorie di attività trattate

1. Il Registro delle categorie di attività trattate da ciascun Responsabile di cui al precedente art. 4, reca le seguenti informazioni:

- a) il nome ed i dati di contatto del Responsabile del trattamento e del RPD;
- b) le categorie di trattamenti effettuati da ciascun Responsabile: raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione, raffronto, interconnessione, limitazione, cancellazione, distruzione, profilazione, pseudonimizzazione, ogni altra operazione applicata a dati personali;
- c) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
- d) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate, come da precedente art.6.

2. Il registro è tenuto dal Responsabile del trattamento presso gli uffici della propria struttura organizzativa in forma telematica o cartacea, secondo lo schema allegato B al presente regolamento.

3. Il Responsabile del trattamento può decidere di affidare al RPD il compito di tenere il Registro, sotto la responsabilità del medesimo Responsabile.

#### Art.9

##### Valutazioni d'impatto sulla protezione dei dati

1. Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e la libertà delle persone fisiche, il Titolare, prima di effettuare il trattamento, deve effettuare una valutazione dell'impatto del medesimo trattamento (DPIA) al fine di valutare le misure tecniche ed organizzative adottate, il rapporto e la finalità dello



Via Pietro Leopoldo 33/34 - 51028 San Marcello Pistoiese - [unionecomuniappenninopistoiese@pec.it](mailto:unionecomuniappenninopistoiese@pec.it)  
C.F. : 90054180472

stesso trattamento. La DPIA è una procedura che permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi.

2. Ai fini della decisione di effettuare o meno la DPIA si tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione come redatti e pubblicati dal Garante Privacy ai sensi dell'art. 35, pp. 4-6, RGDP.

3. La DPIA è effettuata in presenza di un rischio elevato per i diritti e la libertà delle persone fisiche. Fermo restando quanto indicato dall'art. 35, p. 3, RGDP, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono i seguenti:

a) trattamenti valutativi o di scoring, compresa la profilazione e attività predittive, concernenti aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato;

b) decisioni automatizzate che producono significativi effetti giuridici o di analogia natura, ossia trattamenti finalizzati ad assumere decisioni su interessati che producano effetti giuridici sulla persona fisica ovvero che incidono in modo analogo significativamente su dette persone fisiche;

c) monitoraggio sistematico, ossia trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di un'area accessibile al pubblico;

d) trattamenti di dati sensibili o dati di natura estremamente personale, ossia le categorie particolari di dati personali di cui all'art. 9, RGDP;

e) trattamenti di dati su larga scala, tenendo conto: del numero di soggetti interessati del trattamento, in termini numerici o di percentuali rispetto alla popolazione di riferimento; volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; durata o persistenza dell'attività di trattamento; ambito geografico dell'attività di trattamento;

f) combinazione o raffronto di insiemi di dati, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;

g) dati relativi a interessati vulnerabili, ossia ogni interessato particolarmente vulnerabile e meritevole di specifica tutela per il quale si possa identificare una situazione di disequilibrio nel rapporto con il Titolare del trattamento, come i dipendenti dell'Ente, soggetti con patologie psichiatriche, richiedenti asilo, pazienti, anziani e minori;

h) utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;



Via Pietro Leopoldo 10/3/A - 51028 San Marcello Pistoiese - [unionecomuniappenninopistoiese@pec.it](mailto:unionecomuniappenninopistoiese@pec.it)  
C.F. : 50054130472

l) tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

Nel caso in cui un trattamento soddisfi almeno due dei criteri sopra indicati occorre, in via generale, condurre una DPIA, salvo che il Titolare ritenga motivatamente che non può presentare un rischio elevato; il Titolare può motivatamente ritenere che per un trattamento che soddisfa solo uno dei criteri di cui sopra occorre comunque la conduzione di una DPIA.

4. Il Titolare garantisce l'effettuazione della DPIA ed è responsabile della stessa. Il Titolare può affidare la conduzione materiale della DPIA ad un altro soggetto, interno o esterno all'Unione.

Il Titolare deve consultarsi con il RPD anche per assumere la decisione di effettuare o meno la DPIA; tale consultazione e le conseguenti decisioni assunte dal Titolare devono essere documentate nell'ambito della DPIA. Il RPD monitora lo svolgimento della DPIA.

Il Responsabile del trattamento deve assistere il Titolare nella conduzione della DPIA fornendo ogni informazione necessaria.

Il responsabile della sicurezza dei sistemi informativi, se nominato, e/o l'ufficio competente per detti sistemi, forniscono supporto al Titolare per lo svolgimento della DPIA.

5. Il RPD può proporre lo svolgimento di una DPIA in rapporto a uno specifico trattamento, collaborando al fine di mettere a punto la relativa metodologia, definire la qualità del processo di valutazione del rischio e l'accettabilità o meno del livello di rischio residuale.

Il responsabile della sicurezza dei sistemi informativi, se nominato, e/o l'ufficio competente per detti sistemi, possono proporre di condurre una DPIA in relazione a uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.

6. La DPIA non è necessaria nei casi seguenti:

- se il trattamento non può comportare un rischio elevato per i diritti o le libertà di persone fisiche ai sensi dell'art. 35, p. 1, RGDP;
- se la natura, l'ambito, il contesto e le finalità del trattamento sono simili a quelli di un trattamento per il quale è già stata condotta una DPIA. In questo caso si possono utilizzare i risultati della DPIA svolta per l'analogo trattamento;
- se il trattamento è stato sottoposto a verifica da parte del Garante Privacy prima del maggio 2018 in condizioni specifiche che non hanno subito modifiche;
- se un trattamento trova la propria base legale nella vigente legislazione che disciplina lo specifico trattamento, ed è già stata condotta una DPIA all'atto della definizione della base giuridica suddetta.



Via Pietro Leopoldo 10/24 - 51028 San Marcello Pistoiese – [unionecomuniappenninici@pec.it](mailto:unionecomuniappenninici@pec.it)  
C.F. : 90054130472

Non è necessario condurre una DPIA per quei trattamenti che siano già stati oggetto di verifica preliminare da parte del Garante della Privacy o da un RDP o che proseguano con le stesse modalità oggetto di tale verifica. Inoltre, occorre tener conto che le autorizzazioni del Garante Privacy basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite ed abrogate.

7. La DPIA è condotta prima di dar luogo al trattamento, attraverso i seguenti processi:

a) descrizione sistematica del contesto, dei trattamenti previsti, delle finalità del trattamento e tenendo conto dell'osservanza di codici di condotta approvati. Sono altresì indicati: i dati personali oggetto del trattamento, i destinatari e il periodo previsto di conservazione dei dati stessi; una descrizione funzionale del trattamento; gli strumenti coinvolti nel trattamento dei dati personali (hardware, software, reti, persone, supporti cartacei o canali di trasmissione cartacei);

b) valutazione della necessità e proporzionalità dei trattamenti, sulla base:

- delle finalità specifiche, esplicite e legittime;
- della liceità del trattamento;
- dei dati adeguati, pertinenti e limitati a quanto necessario;
- del periodo limitato di conservazione;
- delle informazioni fornite agli interessati;
- del diritto di accesso e portabilità dei dati;
- del diritto di rettifica e cancellazione, di opposizione e limitazione del trattamento;
- dei rapporti con i responsabili del trattamento;
- delle garanzie per i trasferimenti internazionali di dati;
- consultazione preventiva del Garante privacy;

c) valutazione dei rischi per i diritti o le libertà degli interessati, valutando la particolare probabilità e gravità dei rischi rilevati. Sono determinati l'origine, la natura, la particolarità e la gravità dei rischi e, in modo più specifico, di ogni singolo rischio (accesso illegittimo, modifiche indesiderate, indisponibilità dei dati) dal punto di vista degli interessati;

d) individuazione delle misure previste per affrontare ed attenuare i rischi, assicurare la protezione dei dati personali e dimostrare la conformità del trattamento con il RGPD, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

8. Il Titolare può raccogliere le opinioni degli interessati o dei loro rappresentanti, se gli stessi possono essere preventivamente individuati. La mancata consultazione è specificatamente motivata, così come la decisione assunta in senso difforme dall'opinione degli interessati.

9. Il Titolare deve consultare il Garante Privacy prima di procedere al trattamento se la risultanza della DPIA indica l'esistenza di un rischio sostanziale elevato. Il Titolare consulta il Garante Privacy anche nel caso in cui la propria valutazione stabilisce l'esistenza di un rischio alto.



Via Pietro Leopoldo 10/24 - 11028 San Marcello Piemonte - [unione.comuniappenninopiemonese@pec.it](mailto:unione.comuniappenninopiemonese@pec.it)  
C.F. : 96054130472

ottenere la previa autorizzazione della medesima autorità, per trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale ed alla sanità pubblica.

10. La DPIA deve essere effettuata - con eventuale riasseme delle valutazioni condotte - anche per i trattamenti in corso che possano presentare un rischio elevato per i diritti o le libertà delle persone fisiche, nel caso in cui siano intervenute variazioni dei rischi originali tenuto conto della natura, dell'ambito, del contesto e delle finalità del medesimo trattamento.

#### Art. 10

#### 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'Unione.

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 GDPR, 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;
- diffusione non autorizzata della pseudonimizzazione;
- perdita della vita o integrità fisica;



Via Pietro Leopoldo 10/24 - 53028 San Marcello Pistoiese - [unionecomuniappenninoristoiесе@pec.it](mailto:unionecomuniappenninoristoiесе@pec.it)  
C.F. : 90054130472

- 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 verificatasi. 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 *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.

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.15

Rinvio

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



**QUESTIONARIO SULLA PROTEZIONE DEI DATI PERSONALI E SULLA SICUREZZA**

BUREAU CONSULENTI S.p.A. P.zza Mazzini, 10		Cognome del richiedente	
Indirizzo		Indirizzo	
N. telefono		N. telefono	
Mail		Mail	
PEC		PEC	
Delegato del Titolare (eventuale)		Esponente professionale	
Indirizzo		Indirizzo	
N. telefono		N. telefono	
Mail		Mail	
PEC		PEC	
		Registro tenute di	
		Data di creazione	
		Ultimo aggiornamento	
		N. schede compilate	
		Prossima revisione	

n. ordine	Descrizione	TRATTAMENTO			TRASFERIMENTI Paesi terzi, organi int.li (eventuale)	SICUREZZA Misure tecniche ed organizzative adottate
		Finalità	Categorie	Eventuale diverso Titolare o Comitolare		



COMUNICAZIONE DI DELIBERAZIONE

Il presente documento, ai sensi e per gli effetti dell'art. 124 della legge n. 267/00, è  
avuto come per 10 giorni consecutivi a data di esecuzione del presente (dieci) giorni dall'effettuazione stessa.

È copia conforme all'originale, rilasciata in carta libera e per uso amministrativo, composta di n. 4 pagine.

San Marcello Pistoiese, il 12/05/2015

Il Segretario



ATTESTAZIONE ESECUTIVITA' E TRASMISSIONE DELIBERA

Deliberazione divenuta esecutiva a seguito di pubblicazione all'albo pretorio in data \_\_\_\_\_

Deliberazione dichiarata immediatamente eseguibile ai sensi di Legge

Trasmessa ai Responsabili di Area

San Marcello Pistoiese, il 12/05/2015

Il Segretario

