



COMUNE DI RADICONDOLI
Provincia di SIENA

COPIA

DELIBERAZIONE DI GIUNTA COMUNALE
Numero 64 del 18/05/2018

OGGETTO: ADEMPIMENTI REGOLAMENTO UE 2016/679 RELATIVO ALLA PROTEZIONE PERSONE FISICHE TRATTAMENTO DEI DATI PERSONALI - ADESIONE AL PERCORSO AREA VASTA E DETERMINAZIONI

L'anno duemiladiciotto e questo giorno diciotto del mese di maggio alle ore 08.45 nella Sede Comunale, si è riunita la Giunta Comunale nelle persone dei Sigg.:

			Presenti	Assenti
1	BRAVI EMILIANO	Sindaco	X	
2	FIORENZANI FERNANDO	Vice Sindaco	X	
			2	0

Presiede l'adunanza il Sig: BRAVI EMILIANO in qualità di SINDACO assistito dal Segretario C/le TOSCANO FABIO incaricato della redazione del presente verbale.

Pareri ai sensi dell'art. 49 comma 1[^] del Decreto Legislativo n° 267 del 18.08.2000

Il **Responsabile del Settore** esprime parere Favorevole in ordine alle Regolarità Tecnica.
Data 16/05/2018 Il Responsabile Fto Muzzi Stefania

Il **Responsabile del Settore Amministrativo-Contabile** esprime parere Favorevole in ordine alla Regolarità Contabile
Data 16/05/2018 Il Responsabile Fto Muzzi Stefania

Il presente verbale viene letto, approvato e sottoscritto.

IL SINDACO
Fto BRAVI EMILIANO

IL SEGRETARIO COMUNALE
Fto TOSCANO FABIO

ATTESTATO DI PUBBLICAZIONE

La presente delibera è stata pubblicata all'Albo on line di questo Comune in data 28/05/2018 per rimanervi 15 gg consecutivi al n° ed è stata contestualmente comunicata ai capigruppo con protocollo n. Li 28/05/2018

IL RESPONSABILE DELLA PUBBLICAZIONE

IL SEGRETARIO COMUNALE
Fto TOSCANO FABIO

CERTIFICATO DI ESECUTIVITA'

- Immediatamente esecutiva

La presente deliberazione è **esecutiva** in data 18/05/2018 :

IL SEGRETARIO COMUNALE
Fto TOSCANO FABIO

Copia conforme all'originale in carta libera per uso amministrativo.
28/05/2018

IL SEGRETARIO COMUNALE
Toscano Fabio



COMUNE DI RADICONDOLI
Provincia di SIENA

PROPOSTA DI DELIBERAZIONE DELLA GIUNTA COMUNALE

N.72 del 16/05/2018

Ufficio: PROPOSTE DI GIUNTA
COMUNALE
Responsabile del Procedimento: Muzzi Stefania

Assessore: Emiliano Bravi

**OGGETTO: ADEMPIMENTI REGOLAMENTO UE 2016/679 RELATIVO ALLA
PROTEZIONE PERSONE FISICHE TRATTAMENTO DEI DATI PERSONALI - ADESIONE
AL PERCORSO AREA VASTA E DETERMINAZIONI**

Pareri ai sensi dell' art. 49 comma 1^ del Decreto Legislativo n. 267 del 18.08.2000

Il Responsabile del Settore esprime parere Favorevole in ordine alla Regolarità Tecnica.
Data 16/05/2018 Il Responsabile: Fto Muzzi Stefania

**Il Responsabile del Settore Amministrativo-Contabile parere Favorevole in ordine alla
Regolarità Contabile / Attestazione Copertura Finanziaria**
Data 16/05/2018 Il Responsabile: Fto Muzzi Stefania



COMUNE DI RADICONDOLI
Provincia di SIENA

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 funzionamento e organizzazione degli uffici e dei servizi, 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;

CONSTATATO che il regolamento introduce regole più chiare in materia di informativa e consenso, definisce limiti al trattamento automatizzato dei dati personali, pone le basi per l'esercizio di nuovi diritti, stabilisce criteri rigorosi per il trasferimento dei dati al di fuori dell'UE e per i casi di violazione dei dati personali (data breach);

EVIDENZIATO che il GDPR ridisegna, in particolare, il ruolo, i compiti e le responsabilità del Titolare e del Responsabile del trattamento dei dati personali in relazione ai nuovi principi e strumenti introdotti dallo stesso e individua la nuova figura del responsabile della protezione dei dati (RPD);

ATTESO che l'Ente può avvalersi del soggetto idoneo alla nomina di RPD individuato dal Consorzio Terreclabate, nell'ambito dei servizi strumentali alle proprie attività e dello svolgimento esternalizzato di funzioni amministrative di competenza dello stesso Ente inerenti alle attività di progettazione, realizzazione, e fornitura di reti ed erogazione di servizi I.C.T. (Information and Communication Technology) nell'interesse e per conto delle amministrazioni consorziate;

CONSIDERATO che la normativa europea non sarà fonte unica in materia, residuando in capo a ciascuno degli Stati membri dell'Unione una potestà normativa limitata (v. artt. 23 e 17, par. 3, per quanto riguarda il diritto alla cancellazione/"oblio", art. 83 per i trattamenti di natura giornalistica e art. 89 sui trattamenti per finalità di ricerca scientifica o storica o di statistica) e che la violazione della legislazione in materia di dati personali da parte degli Enti pubblici costituisce condotta gravemente colposa fonte di responsabilità personale che comporta l'obbligo del risarcimento del danno erariale quantificato in misura pari alla sanzione amministrativa pecuniaria irrogata dal Garante, ai sensi degli



COMUNE DI RADICONDOLI
Provincia di SIENA

artt. 161-166 del citato Codice (Corte dei Conti-Sardegna, Sez. giurisdiz., sentenza 8 marzo-12 aprile 2018, n. 73);

ATTESO che la disciplina normativa in materia di trattamento e protezione dei dati personali è attualmente contenuta nell'apposito Codice, emanato con D.Lgs. n. 196 del 2003 e s.m.i;

RAVVISATA la necessità di adottare un regolamento interno che recepisca ed attui le disposizione del Regolamento UE, in conformità alle attività di Studio e di analisi svolte da ANCI, secondo gli indirizzi emanati dal Garante Privacy e dalle Linee Guida del Gruppo Lavoro Articolo 29;

VISTO lo schema di Regolamento allegato A);

ATTESA la propria competenza trattandosi di disciplina integrativa del vigente Regolamento sull'ordinamento degli uffici e servizi ai sensi dell'art. 48 comma III del d.lgs. 267/2000, di cui costituisce specifica appendice;

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

RITENUTO pertanto di aderire al percorso per l'assolvimento degli obblighi previsti dal Regolamento UE 2016/679 in materia di protezione dati personali, riconoscendo la Provincia di Siena quale Ente attuatore in quanto esercente la funzione di assistenza tecnico amministrativa ai Comuni ai sensi dell'art. 1 comma 85 lettera d) della legge n. 56 del 7/04/2014, in collaborazione e con il supporto tecnico del Consorzio Terrecablate come previsto dall'art. 2 comma I lettera a) del vigente Statuto del Consorzio stesso;

PRECISATO che ai sensi dell'art. 5 del d. lgs. 50/2016 il Consorzio Terrecablate è stato iscritto nell'elenco delle amministrazioni aggiudicatrici che operano mediante affidamenti in house con domanda di iscrizione n. 838 del 24/04/2018;

VISTI i pareri di regolarità tecnica del dirigente/responsabile e di regolarità contabile del responsabile del servizio economico – finanziario, ai sensi dell'art. 49 del Tuel;

Propone

1. di aderire al percorso per l'assolvimento degli obblighi previsti dal Regolamento UE 2016/679 in materia di protezione dati personali, riconoscendo la Provincia di Siena quale Ente attuatore in quanto esercente la funzione di assistenza tecnico amministrativa ai Comuni ai sensi dell'art. 1 comma 85 lettera d) della legge n. 56 del 7/04/2014, in collaborazione e con il supporto tecnico del Consorzio Terrecablate come previsto dall'art. 2 comma I lettera a) del vigente Statuto del Consorzio;
2. di approvare il Regolamento attuativo del Regolamento UE 2016/679 in materia di protezione dati personali (allegato A parte integrante e sostanziale del presente atto), che consta di n.10 articoli e n. 3 schede che viene allegato al presente atto per costituirne parte integrante e sostanziale, che si configura quale disciplina integrativa/appendice del vigente Regolamento sull'ordinamento degli uffici e servizi ai sensi dell'art. 48 comma III del d.lgs. 267/2000;
3. di approvare il progetto di adeguamento normativo e ripartizione costi di cui all'allegato B (adeguato per quel che concerne il numero di postazioni fisse riferite al Comune di Radicondoli) parte integrante e sostanziale del presente provvedimento, dando atto che le somme verranno reperite al Cap.lo 115010 " Servizio aggiornamento documenti privacy" che offre la necessaria disponibilità;



COMUNE DI RADICONDOLI
Provincia di SIENA

4. di precisare che restano ferme 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).
5. di dare mandato, al Consorzio Terrecablate di indire la procedura per l'individuazione del soggetto idoneo alla nomina di Responsabile della Protezione Dati secondo le disposizioni vigenti;
6. di demandare altresì al Consorzio Terrecablate e alla Provincia di Siena tutte le azioni necessarie all'attuazione di quanto previsto nel progetto di adeguamento normativo e ripartizione costi di cui all'allegato B sopra approvato;
7. di dare atto che con successivi provvedimenti, si procederà secondo la disciplina contenuta nel presente atto ed in conformità a quanto stabilito nel Regolamento UE 2016/679 ed in particolare spetterà:

alla Provincia di Siena:

- il coordinamento giuridico - amministrativo e la predisposizione degli atti propedeutici a:
- alla nomina dei Responsabili del trattamento;
 - alla designazione del Responsabile della Protezione Dati;

al Consorzio Terrecablate:

- l'esecuzione della procedura di individuazione del Responsabile della Protezione Dati;
- all'attività propedeutica all'istituzione dei registri delle attività di trattamento;
- all'attività propedeutica all'aggiornamento della documentazione in essere nell'Ente in relazione ai trattamenti dei dati personali;

ad ogni singolo Ente:

- la nomina del responsabile del trattamento e la designazione del Responsabile della protezione dati con atti del rappresentante legale secondo la modulistica predisposta dall'amministrazione provinciale con il supporto tecnico del Consorzio Terrecablate, in modo da garantire una costante assistenza tecnico giuridica in ogni fase degli adempimenti richiesti;
- la compartecipazione al percorso per € 2.800,00, secondo la tabella di ripartizione di cui all'allegato B sopra approvato;

8. di stabilire che l'approvazione del presente atto, comprensivo dell'allegato regolamento, oltre a valore dispositivo, assume anche valore negoziale di accordo di collaborazione ai sensi dell'art. 15 della legge 241/1990;

9. di dichiarare la presente immediatamente eseguibile ex art. 134, comma 4, Tuel, vista la scadenza prevista dalla legge del 25/05/2018.



COMUNE DI RADICONDOLI
Provincia di SIENA

IL SINDACO

Aprè la discussione sul punto in ordine del giorno.

Uditi gli interventi, si mette in votazione la proposta.

LA GIUNTA COMUNALE

Esaminata la proposta;

Acquisito i pareri di cui all'art. 49 del Decreto Leg.vo n° 267/2000;

AD UNANIMITA' di voti espressi in forma palese dagli assessori presenti,

Delibera

- 1) Di approvare la proposta in ordine del giorno.
- 2) Di dichiarare con separata votazione, il presente atto immediatamente eseguibile, ai sensi dell' art. 134 comma 4 del Decreto Leg.vo n° 267/2000, ad unanimità di voti.

Esaurito l'ordine del giorno la seduta è tolta alle ore 9,00.

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

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 e disposizioni finali

Allegati

A) schema di registro attività di trattamento

B) schema di registro categorie attività di trattamento

C) schema di registro unico di trattamento

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), relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione di tali dati.

Art.2. Titolare del trattamento

1. L'Ente, rappresentato ai fini previsti dal RGPD dal Sindaco/Presidente, è il Titolare del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee (di seguito indicato con "Titolare"). Il titolare può delegare le relative funzioni al Segretario/ Dirigente/Responsabile P.O. in possesso di adeguate competenze.
2. Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 del 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.
4. 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 del GDPR, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio.
5. Gli interventi necessari per l'attuazione delle misure sono considerati nell'ambito del documento unico di programmazione (DUP) e di piano esecutivo di gestione (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 le libertà delle persone fisiche.
6. Il Titolare adotta misure appropriate per fornire all'interessato:
 - a) le informazioni indicate dall'art. 13 del GDPR, qualora i dati personali siano raccolti presso lo stesso interessato;
 - b) le informazioni indicate dall'art. 14 del GDPR, qualora i dati personali non stati ottenuti presso lo stesso interessato.
7. 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 le 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 del GDPR, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento, tenuto conto di quanto indicato dal successivo art. 9.
8. Il Titolare, inoltre, provvede a:
 - a) designare i Responsabili del trattamento nelle persone del Segretario/Dirigenti/Responsabili P.O. 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, come individuato dal consorzio Terrecablate;
 - 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.
9. L'Ente può richiedere alla Provincia di Siena, la raccolta ed elaborazione di dati, assistenza tecnico-amministrativa, nell'ambito della funzione fondamentale di cui all'art. 1 comma 85, lettera d) della legge n. 56 del 7/04/2014, in collaborazione e con il supporto tecnico del Consorzio Terrecablate.
 10. L'Ente potrà unitamente ad altri due o più titolari del trattamento determinare congiuntamente le finalità e i mezzi del trattamento divenendo contitolari del trattamento Mediante apposito accordo vengono definite le 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 dalla normativa specificatamente applicabile; l'accordo può individuare un punto di contatto comune per gli interessati.
 11. **L'Ente** 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 dimostrarne il concreto rispetto da parte del Titolare e dei Responsabili del trattamento.

Art.3

Finalità del trattamento

1. I trattamenti sono compiuti dall'Ente per le seguenti finalità:
 - a) l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri. Rientrano in questo ambito i trattamenti compiuti per:
 - 1) 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;
 - 2) la gestione dei servizi elettorali, di stato civile, di anagrafe, di leva militare e di statistica;
 - 3) l'esercizio di ulteriori funzioni amministrative per servizi di competenza statale affidate all'Ente in base alla vigente legislazione;
 - b) l'adempimento di un obbligo legale al quale è soggetto l'Ente;
 - c) l'esecuzione di un contratto con soggetti interessati;
 - d) per specifiche finalità diverse da quelle di cui alle lettere precedenti, purché l'interessato esprima il consenso al trattamento.

Art.4

Responsabile del trattamento

1. Per ogni trattamento che debba essere effettuato per conto del Titolare, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative di cui all'art. 6, volte a garantire che i trattamenti siano effettuati in conformità al GDPR.
2. Tali attività vengono svolte con il supporto della Provincia di Siena e del Consorzio Terrecablate, che a tale scopo si impegnano ad informare costantemente ed in maniera preventiva, mettendo a disposizione laddove necessario anche documentazione e schemi di atti, contenenti novità normative e gli adempimenti conseguenti.
3. I dipendenti dell'Ente, quali Responsabili del trattamento, sono designati, mediante decreto di incarico del Sindaco, nel quale sono tassativamente disciplinati:
 - a) la materia trattata, la durata, la natura e la finalità del trattamento o dei trattamenti assegnati;
 - b) il tipo di dati personali oggetto di trattamento e le categorie di interessati;
 - c) gli obblighi ed i diritti del Titolare del trattamento.

4. Il Titolare può avvalersi, per il tramite del Consorzio Terrecablate ai fini del 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.
5. Gli atti che disciplinano il rapporto tra il Titolare ed il Responsabile del trattamento devono in particolare contenere quanto previsto dall'art. 28, **comma 3 del GDPR**; tali atti possono anche basarsi su clausole contrattuali tipo adottate dal Garante per la protezione dei dati personali oppure dalla Commissione europea.
6. È 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.
7. 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.
8. 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 od abbia un adeguato obbligo legale di riservatezza.
9. 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, analiticamente specificati per iscritto nell'atto di designazione, ed in particolare provvede:
 - a) alla tenuta del registro delle categorie di attività di trattamento svolte per conto del Titolare;
 - b) all'adozione di idonee misure tecniche e organizzative adeguate per garantire la sicurezza dei trattamenti;
 - c) alla sensibilizzazione ed alla formazione del personale che partecipa ai trattamenti ed alle connesse attività di controllo;
 - d) alla designazione del Responsabile per la Protezione dei Dati (RPD), se a ciò demandato dal Titolare;
 - e) 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;
 - f) 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.5

Responsabile della protezione dati

1. Il Responsabile della protezione dei dati (in seguito indicato con "RPD") è individuato ai sensi di legge, in possesso dei requisiti di capacità tecnico – professionale.
2. L'Ente può avvalersi del soggetto idoneo alla nomina di RPD individuato dal Consorzio Terrecablate, nell'ambito dei servizi strumentali alle proprie attività e dello svolgimento esternalizzato di funzioni amministrative di competenza dello stesso Ente inerenti alle attività di progettazione, realizzazione, e fornitura di reti ed erogazione di servizi I.C.T.

(Information and Communication Technology) nell'interesse e per conto delle amministrazioni interessate.

3. 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 le responsabilità del Titolare e del Responsabile del trattamento. Fanno parte di questi compiti la raccolta di informazioni per individuare i trattamenti svolti, 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 sorvegliarne 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 esternalizzandola; quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi delle persone interessate; se la DPIA sia stata condotta correttamente o meno e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al GDPR;
 - 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) sorvegliare la tenuta dei registri di cui ai successivi artt. 7 e 8.
4. 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:
- a) il RPD è invitato a partecipare alle riunioni di coordinamento dei Segretari/Dirigenti/Responsabili P.O. che abbiano per oggetto questioni inerenti la protezione dei dati personali.
 - b) 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;
 - c) 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;
 - d) il RPD deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.
5. 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 nell'attività da svolgere - ovvero un piano annuale di attività - incentrandola sulle aree di attività che presentano maggiori rischi in termini di protezione dei dati, da comunicare al Titolare ed al Responsabile del trattamento.
6. Il RPD dispone di autonomia e risorse sufficienti a svolgere in modo efficace i compiti attribuiti, tenuto conto delle dimensioni organizzative e delle capacità di bilancio dell'Ente.
 7. La figura di RPD è incompatibile con chi determina le finalità od i mezzi del trattamento; in particolare, risultano con la stessa incompatibili:
 - a) il Responsabile per la prevenzione della corruzione e per la trasparenza;
 - b) il Responsabile del trattamento;
 - c) qualunque incarico o funzione che comporta la determinazione di finalità o mezzi del trattamento.
 8. 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:
 - a) supporto attivo per lo svolgimento dei compiti da parte dei Dirigenti/Responsabili P.O. e degli organi di indirizzo, 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;
 - b) tempo sufficiente per l'espletamento dei compiti affidati al RPD;
 - c) supporto adeguato in termini di risorse finanziarie, infrastrutture (sede, attrezzature, strumentazione) e, ove opportuno, personale; ovvero tramite la costituzione di una U.O., ufficio o gruppo di lavoro RPD (formato dal RPD stesso e dal rispettivo personale);
 - d) 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;
 - e) accesso garantito ai settori funzionali dell'Ente così da fornirgli supporto, informazioni e input essenziali.
 9. 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.
 10. Il RPD non può essere rimosso o penalizzato dal Titolare e dal Responsabile del trattamento per l'adempimento dei propri compiti.
 11. Ferma restando l'indipendenza nello svolgimento di detti compiti, il RPD riferisce direttamente al Titolare od al Responsabile del trattamento.
 12. Nel caso 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'Ente 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, con il supporto tecnico del Consorzio Terrecablate:
 - a) sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; altro);
 - b) misure antincendio; sistemi di rilevazione di intrusione; 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 GDPR 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'Ente 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.
 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 dell'Ente, sezione Amministrazione trasparente, oltre che nella sezione "privacy" eventualmente già presente.
 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'Ente, del Titolare ai sensi del precedente art.2, eventualmente del contitolare 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 misure 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'Ente in forma telematica/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 ai commi precedenti e quelle di cui al successivo art. 8, sostituendo entrambe le tipologie di

registro dagli stessi disciplinati, secondo lo schema allegato C) al presente Regolamento. In tal 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/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 le libertà delle persone fisiche, il Titolare, prima di effettuare il trattamento, deve attuare una valutazione dell'impatto del medesimo trattamento (DPIA) ai sensi dell'art. 35 GDPR, considerati la natura, l'oggetto, il contesto e le finalità dello 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, GDPR.
3. La DPIA è effettuata in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche. Fermo restando quanto indicato dall'art. 35, p. 3, GDPR, 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 analoga 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, GDPR;
 - e) trattamenti di dati su larga scala, tenendo conto: del numero di numero di soggetti interessati dal trattamento, in termini numerici o di percentuale 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;
 - i) tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.
4. 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 occorra comunque la conduzione di una DPIA.
5. 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'Ente.
6. 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.
7. Il Responsabile del trattamento deve assistere il Titolare nella conduzione della DPIA fornendo ogni informazione necessaria.
8. Il responsabile della sicurezza dei sistemi informativi, se nominato, e/o il Consorzio Terrecablate, forniscono supporto al Titolare per lo svolgimento della DPIA.
9. 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.
10. Il responsabile della sicurezza dei sistemi informativi, se nominato, e/o il consorzio Terrecablate, possono proporre di condurre una DPIA in relazione a uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.
11. La DPIA non è necessaria nei casi seguenti:
- a) se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35, p. 1, GDPR;
 - b) 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;
 - c) 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;
 - d) 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.

12. 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 e 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 od abrogate.
13. 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:
 - c) delle finalità specifiche, esplicite e legittime;
 - d) della liceità del trattamento;
 - e) dei dati adeguati, pertinenti e limitati a quanto necessario;
 - f) del periodo limitato di conservazione;
 - g) delle informazioni fornite agli interessati;
 - h) del diritto di accesso e portabilità dei dati;
 - i) del diritto di rettifica e cancellazione, di opposizione e limitazione del trattamento;
 - j) dei rapporti con i responsabili del trattamento;
 - k) delle garanzie per i trasferimenti internazionali di dati;
 - l) consultazione preventiva del Garante privacy;
 - m) valutazione dei rischi per i diritti e 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 o, in modo più specifico, di ogni singolo rischio (accesso illegittimo, modifiche indesiderate, indisponibilità dei dati) dal punto di vista degli interessati;
 - n) 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.
14. 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.
15. Il Titolare deve consultare il Garante Privacy prima di procedere al trattamento se le risultanze della DPIA condotta indicano l'esistenza di un rischio residuale elevato. Il Titolare consulta il Garante Privacy anche nei casi in cui la vigente legislazione stabilisce l'obbligo di consultare e/o 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.
16. La DPIA deve essere effettuata - con eventuale riesame delle valutazioni condotte - anche per i trattamenti in corso che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, nel caso in cui siano intervenute variazioni dei rischi originari 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'Ente.
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 RGPD, sono i seguenti:
 - a) danni fisici, materiali o immateriali alle persone fisiche;
 - b) perdita del controllo dei dati personali;
 - c) limitazione dei diritti, discriminazione;
 - d) furto o usurpazione d'identità;
 - e) perdite finanziarie, danno economico o sociale.
 - f) decifrazione non autorizzata della pseudonimizzazione;
 - g) pregiudizio alla reputazione;
 - h) 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 verificatesi. I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:
 - a) coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
 - b) riguardare categorie particolari di dati personali;
 - c) comprendere dati che possono accrescere ulteriormente i potenziali rischi (ad esempio dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
 - d) 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);
 - e) 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 del GDPR, 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 GDPR.

Art.11

Rinvio e disposizioni finali

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

2. La Provincia di Siena ed il Consorzio Terrecablate, si riservano di proporre entro 12 mesi dall'approvazione del presente Regolamento una eventuale proposta progettuale che oltre a prevedere forme di implementazione delle misure previste dall'attuale regolamentazione, anche una revisione complessiva del percorso, con possibilità di reperire le figure del responsabile della protezione dati all'interno dei soggetti attualmente coinvolti anche previo percorso formativo.
3. Eventuali integrazioni e/o sostituzioni agli allegati apportati su suggerimento ed iniziativa del Responsabile della protezione dati individuato dal Consorzio Terrecablate, non comportano modifiche al presente Regolamento.

Allegato B

GDPR – progetto di adeguamento normativo e ripartizione costi

Il progetto è diviso in due fasi:

Fase n. 1 (interamente gestito dal consorzio Terrecablate): necessario per la fase iniziale del progetto. Di immediata attuazione, comprende un primo essenziale insieme di attività di adempimento degli obblighi previsti del GDPR (Regolamento U.E. N.679/2016):

- a. servizio di "Responsabile Protezione Dati", di seguito anche "RPD", ai sensi degli artt. 37 e segg. del Regolamento UE 2016/679: Nomina RDP in forma congiunta, individuato dal Consorzio Terrecablate;
- b. Definizione di linee guida e fornitura e/o sviluppo software (o altri strumenti) per la compilazione del registro delle attività di trattamento e del registro delle categorie di attività trattate da ciascun Responsabile;
- c. Valutazione di impatto sulla protezione dei dati.

Fase n. 2 : a seguire, e sulla base delle caratteristiche di ogni ente, del suo grado di autonomia e degli aspetti critici emersi nella fase iniziale, comprende le seguenti eventuali attività:

- a. macroanalisi dei flussi informativi legata al trattamento dei dati e supporto al referente di ogni ente nella mappatura dei processi;
- b. supporto alla compilazione del registro dei trattamenti di dati personali e del registro delle categorie di attività con validazione finale;
- c. interventi formativi collettivi per i referenti degli enti;
- d. Valutazione delle vulnerabilità;
- e. Compilazione DPIA;
- f. Identificazione e valutazione degli scostamenti dagli obblighi normativi (*gap analysis*);
- g. elaborazione del piano di adeguamento complessivo, contenente le proposte di miglioramento del livello di sicurezza per i processi che presentano rischi, con stima dei costi (se necessario) e dei tempi previsti, nonché delle attività di monitoraggio.

Le attività relative alla fase n. 2 verranno svolte presso il Consorzio o, quando necessario (e comunque almeno 1 sopralluogo nelle fasi iniziali ed un *audit* finale per la verifica della corretta adozione del sistema di *data protection*), presso la sede dell'ente e dovrà essere ultimata entro 6 mesi dal suo formale avvio. Il Consorzio procederà alle necessarie esternalizzazioni per garantire l'esecuzione della fase n. 2 nel rispetto delle procedure previste dalla legge. A questo seguiranno altri 6 mesi per l'attività di monitoraggio e manutenzione ordinaria del sistema di gestione implementato. La Provincia, per queste attività, garantirà il proprio supporto riservandosi anche di procedere con eventuali esternalizzazioni a norma di legge, con particolare riferimento alle attività di cui alla lettere *a)*, *b)* e *c)* della fase n. 2. In relazione agli interventi formativi la stessa Provincia promuoverà eventuali intese anche con l'Università di Siena e con l'Unione delle Province.

Per l'esecuzione delle attività sopra descritte, a partire dalla fase iniziale, ogni ente deve nominare un referente, la cui figura può coincidere con il responsabile o i responsabili del trattamento di ciascun ente, che dovrà essere caratterizzato da un'ampia visione delle articolazioni del suo Ente e delle attività svolte all'interno.

Dovrà fornire informazioni sulla struttura organizzativa dell'ente e sulle modalità con cui quest'ultimo svolge la propria attività per consentire di individuare le tipologie di dati trattati e le categorie di attività di trattamento; dovrà inoltre interagire con il RDP per permettergli di svolgere la propria attività relativa all'ente.

In particolare sarà chiamato a individuare, sotto la supervisione del RDP e con gli strumenti contemplati nella fase n. 1, contando anche sul supporto della provincia di Siena, la mappatura dei processi per individuare quelli collegati al trattamento dei dati personali e alla compilazione del registro delle attività di trattamento e del registro delle categorie di attività trattate da ciascun Responsabile.

L'attività di RDP verrà svolta ordinariamente presso il Consorzio Terrecablate da un soggetto esterno qualificato e avrà durata pari ad un anno. Il Consorzio metterà a disposizione la propria sede e gli strumenti necessari alla esecuzione della funzione di RDP. Saranno previste visite periodiche programmate presso le sedi degli enti per la verifica della corretta adozione del modello di funzionamento della protezione dei dati oltre a quelle necessarie in seguito a fatti straordinari quali, a titolo meramente semplificato, eventi di *data breach*, visite ispettive, cambiamenti sostanziali della struttura organizzativa, ecc...

La Provincia di Siena, promuovendo anche tavoli tecnici o gruppi di lavoro si occuperà dell'adeguamento della modulistica in uso agli uffici, qualora non conforme alle nuove disposizioni o stesura ex novo della documentazione e avvio della relativa adozione.

Sempre la Provincia faciliterà, in collaborazione con il Consorzio Terrecablate ed i referenti designati da ogni ente e sulle base delle indicazioni fornite dal RDP, un percorso per l'individuazione, tra i processi risultanti dalla mappatura, di quelli che presentano rischi, con una prima valutazione degli stessi in termini di maggiore o minore gravità nonché la mappatura degli incarichi dei soggetti coinvolti nel trattamento e dei livelli di responsabilità, ed eventuale aggiornamento.

Il Consorzio metterà a disposizione le proprie conoscenze relative all'infrastruttura informatica utilizzata dagli enti nelle fasi di:

- macroanalisi dei flussi informativi legata al trattamento dei dati e supporto al referente di ogni ente nella mappatura dei processi;
- di valutazione delle vulnerabilità;
- stesura del piano di adeguamento.

Si farà carico, inoltre, di attivare e rendere disponibili gli strumenti informatici per l'automatizzazione della raccolta e gestione dei dati per la stesura del registro delle attività di trattamento e del registro delle categorie di attività trattate da ciascun ente.

Il costo stimato del progetto, comprensivo delle due fasi sopra descritte per ogni ente, è il seguente:

ENTE	totale PdL	fascia	Fase n. 1 (€/anno)	Fase n. 2 (€)
AMM.NE PROVINCIALE	125	E	2000	6500
ABBADIA S.SALVATORE	38	C	1200	2500
ASCIANO				
BUONCONVENTO	23	B	900	2000
CASOLE D'ELSA				
CASTELLINA IN CHIANTI	22	B	900	2000
CASTELNUOVO BERARDENGA	37	C	1200	2500
CASTIGLIONE D'ORCIA	18	A	800	2000
CETONA	27	B	900	2000
CHIANCIANO TERME	56	D	1500	4500
CHIUSDINO				
CHIUSI	48	C	1200	2500
COLLE DI VAL D'ELSA				
GAIOLE IN CHIANTI	18	A	800	2000
MONTALCINO	34	C	1200	2500
MONTEPULCIANO	72	D	1500	4500
MONTERIGGIONI	44	C	1200	2500
MONTERONI D'ARBIA	33	C	1200	2500
MONTICIANO				
MURLO				
PIANCASTAGNAIO	18	A	800	2000
PIENZA	17	A	800	2000
POGGIBONSI	147	E	2000	6500
RADDA IN CHIANTI	19	A	800	2000
RADICOFANI	12	A	800	2000
RADICONDOLI	10	A	800	2000
RAPOLANO TERME	21	B	900	2000
SAN CASCIANO DEI BAGNI	19	A	800	2000
SAN GIMIGNANO	55	D	1500	4500
SAN QUIRICO D'ORCIA	18	A	800	2000
SARTEANO	44	C	1200	2500
SIENA	630	G	4000	12000
SINALUNGA	60	D	1500	4500
SOVICILLE				
TORRITA DI SIENA	33	C	1200	2500
TREQUANDA	15	A	800	2000
UNIONE DEI COMUNI AMIATA VALDORCIA	30	B	900	2000
UNIONE DEI COMUNI VALDICHIANA SENESE	47	C	1200	2500
CONSORZIO TERRECABLATE	8	A	800	2000
TERRE DI SIENA LAB	8	A	800	2000
	1655		38900	99500

N.B. Il percorso sarà effettivamente attuabile se ciascun Ente fornirà idoneo supporto mettendo a disposizione uno o più referenti in modo da facilitare l'espletamento del servizio.

Per le attività della fase n. 2 si precisa che i costi sono solo stimati e che probabilmente si potranno avere delle economie a seguito delle procedure di scelta del contraente e del supporto soprattutto in ambito formativo che la Provincia di Siena riuscirà ad attivare. Pertanto non si esclude che a rendicontazione le spese per ciascun Comune potranno essere inferiori a quelle stimate.